Configuration Guide for Cisco Secure ACS 4.2

February 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-14390-02

Configuration Guide for Cisco Secure ACS 4.2

CONTENTS

Preface

Audience

This guide is for security administrators who use Cisco Secure Access Control Server (ACS), and who set up and maintain network and application security.

Organization

This document contains:

- Chapter 1, "Overview of ACS Configuration"—Provides an overview of ACS configuration, including a summary of configuration steps and configuration flowchart that show the sequence of configuration steps.
- Chapter 2, "Deploy the Access Control Servers"—Describes factors to consider when deploying ACS, including the access type, network topology, and whether database synchronization and replication are required.
- Chapter 3, "Configuring New Features in ACS 4.2"—Describes how to configure the most important new features in ACS 4.2.
- Chapter 4, "Using RDBMS Synchronization to Create dACLs and Specify Network Configuration"—Describes how to configure new RDBMS synchronization features in ACS 4.2 and run RDBMS Sync remotely on the ACS Solution Engine.
- Chapter 5, "Password Policy Configuration Scenario"—Describes how to configure Sarbanes-Oxley (SOX) support when adding administrators.
- Chapter 6, "Agentless Host Support Configuration Scenario"—Describes how to configure ACS for agentless host support (MAC authentication bypass).
- Chapter 7, "PEAP/EAP-TLS Configuration Scenario"—Describes how to configure ACS for PEAP/EAP-TLS support.
- Chapter 8, "Syslog Logging Configuration Scenario"—Describes how to configure ACS to log syslog messages.
- Chapter 9, "NAC Configuration Scenario"—Describes how to configure ACS in a Cisco Network Admission Control (NAC) and Microsoft Network Access Protection (NAP) environment.
- "Glossary"—Lists common terms used in ACS.

Conventions

This document uses the following conventions:

Item	Convention
Commands, keywords, special terminology, and options that should be selected during procedures	**boldface** font
Variables for which you supply values and new or important terminology	*italic* font
Displayed session and system information, paths and file names	`screen` font
Information you enter	**`boldface screen`** font
Variables you enter	*italic screen* font
Menu items and button names	**boldface** font
Indicates menu items to select, in the order you select them.	**Option > Network Preferences**

Tip Identifies information to help you get the most benefit from your product.

Note Means *reader take note*. Notes identify important information that you should reflect upon before continuing, contain helpful suggestions, or provide references to materials not contained in the document.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage, loss of data, or a potential breach in your network security.

Warning **Identifies information that you must heed to prevent damaging yourself, the state of software, or equipment. Warnings identify definite security breaches that will result if the information presented is not followed carefully.**

Product Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

Table 1 describes the product documentation that is available.

Table 1 ACS 4.2 Documentation

Document Title	Available Formats
Documentation Guide for Cisco Secure ACS Release 4.2	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/roadmap/DGuide42.html
Release Notes for Cisco Secure ACS Release 4.2	On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/release/notes/ACS42_RN.html
Configuration Guide for Cisco Secure ACS Release 4.2	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/configuration/guide/acs42_config_guide.html
Installation Guide for Cisco Secure ACS for Windows Release 4.2	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html
Installation Guide for Cisco Secure ACS Solution Engine Release 4.2	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/SE42.html
Configuration Guide for Cisco Secure ACS 4.2	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/user/guide/ACS4_2UG.html
Regulatory Compliance and Safety Information for the Cisco Secure ACS Solution Engine Release 4.2	• Shipped with product. • PDF on the product CD-ROM. • On Cisco.com: • http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/regulatory/compliance/RCSI_42.html
Installation and Configuration Guide for Cisco Secure ACS Remote Agents Release 4.2	• On Cisco.com: • http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/remote_agent/rmag42.html
Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.2	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/device/guide/sdt42.html

Table 1 ACS 4.2 Documentation (continued)

Document Title	Available Formats
Installation and User Guide for Cisco Secure ACS User-Changeable Passwords	• On Cisco.com: http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/user_passwords/ucp42.html
Troubleshooting Guide for Cisco Secure Access Control Server	• On Cisco.com http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/trouble/guide/ACS_Troubleshooting.html
Online Documentation	In the ACS HTML interface, click **Online Documentation**.
Online Help	In the ACS HTML interface, online help appears in the right-hand frame when you are configuring a feature.

Related Documentation

Note We sometimes update the printed and electronic documentation after original publication. Therefore, you should also review the documentation on Cisco.com for any updates.

A set of white papers about ACS are available on Cisco.com at:

http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/index.shtml

For information on Network Admission Control, various NAC components, and ACS see:

http://www.cisco.com/go/NAC

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

CHAPTER 1

Overview of ACS Configuration

This chapter describes the general steps for configuring Cisco Secure Access Control Server, hereafter referred to as ACS, and presents a flowchart showing the sequence of steps.

Note If you are configuring ACS to work with Microsoft clients in a Cisco Network Access Control/Microsoft Network Access Protection (NAC/NAP) network, refer to Chapter 9, "NAC Configuration Scenario."

This chapter contains:

Summary of Configuration Steps

To configure ACS:

Step 1 Plan the ACS Deployment.

Determine how many ACS servers you need and their placement in the network.

For detailed information, see Chapter 2, "Deploy the Access Control Servers."

Step 2 Install the ACS Servers.

Install the ACS servers as required. For detailed installation instructions, refer to:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.2*, available on Cisco.com at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html

- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*, available on Cisco.com at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/ACS_42_SE_install.html

Step 3 Configure Additional Administrators.

When you install the Windows version of ACS, there are initially no administrative users. When you install Cisco Secure ACS Solution Engine (ACS SE), there is initially one administrator.

To set up additional administrative accounts:

a. Add Administrators.

b. For each administrator, specify administrator privileges.

c. As needed, configure the following optional administrative policies:

- **Access Policy**—Specify IP address limitations, HTTP port restrictions, and secure socket layer (SSL) setup.
- **Session Policy**—Specify timeouts, automatic local logins, and response to invalid IP address connections.
- **Password Policy**—Configure the password policy for administrators.

For detailed information, see Chapter 5, "Password Policy Configuration Scenario."

Step 4 Configure the Web Interface:

a. Add AAA clients and specify the authorization protocols that the clients will use.

b. Click **Interface Configuration**.

c. On the Interface Configuration page, configure the interface to include one or more of:

- **RADIUS Configuration Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."
- **TACACS+ Configuration Options**—For detailed information, see "Displaying TACACS+ Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."
- **Advanced Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."
- **Customized User Options**—For detailed information, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."

Step 5 Configure Basic ACS System Settings:

a. Click **System Configuration**.

b. Configure:

- Service Control
- Logging
- Date Format Control
- Local Password Management
- ACS Backup
- ACS Restore
- ACS Service Management
- (optional) IP Pools Server
- (optional) IP Pools Address Recovery

For detailed instructions, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."

Step 6 Configure Users:

a. As required for your network security setup, configure users. You can configure users:

- Manually, by using the ACS web interface
- By using the **CSUtil** utility to import users from an external database

  - By using database synchronization
  - By using database replication

For detailed instructions, see "Displaying RADIUS Configuration Options" in Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "Using the Web Interface."

Step 7 Configure Certificates.

This step is required if you are using EAP-TLS, Secure Sockets Layer (SSL), or Cisco Network Admission Control (NAC).

For detailed instructions, see Step 3: Install and Set Up an ACS Security Certificate, page 6-6.

Step 8 Configure Global Authentication Settings.

Configure the security protocols that ACS uses to authenticate users. You can configure the following global authentication methods:

- PEAP
- EAP-FAST
- EAP-TLS
- LEAP
- EAP-MD5
- Legacy authentication protocols, such as MS-CHAP Version 1 and Version 2

For detailed instructions, see "Global Authentication Setup" in Chapter 8 of the *User Guide for Cisco Secure ACS 4.2*, "System Configuration: Authentication and Certificates."

Step 9 Configure Shared Profile Components.

You can configure the following shared profile components:

- Downloadable IP ACLs
- Network Access Filtering
- RADIUS Authorization Components
- Network Access Restrictions
- Command Authorization Sets

For detailed instructions, see Chapter 3 of the *User Guide for Cisco Secure ACS 4.2*, "Shared Profile Components."

Step 10 Set Up Network Device Groups.

You can set up network device groups to simplify configuration of common devices. For detailed information, see the *User Guide for Cisco Secure ACS 4.2*.

Step 11 Add AAA clients.

You can add RADIUS clients or TACACS+ clients. For detailed instructions, see Step 2: Configure a RADIUS AAA Client, page 6-5.

Step 12 Set Up User Groups.

Set up user groups to apply common configuration settings to groups of users. For detailed instructions, see Chapter 2 of the *User Guide for Cisco Secure ACS 4.2*, "User Group Management."

Step 13 Configure Posture Validation.

If you are using ACS with NAC, configure posture validation.

Step 14 Set Up Network Access Profiles.

If required, set up Network Access Profiles.

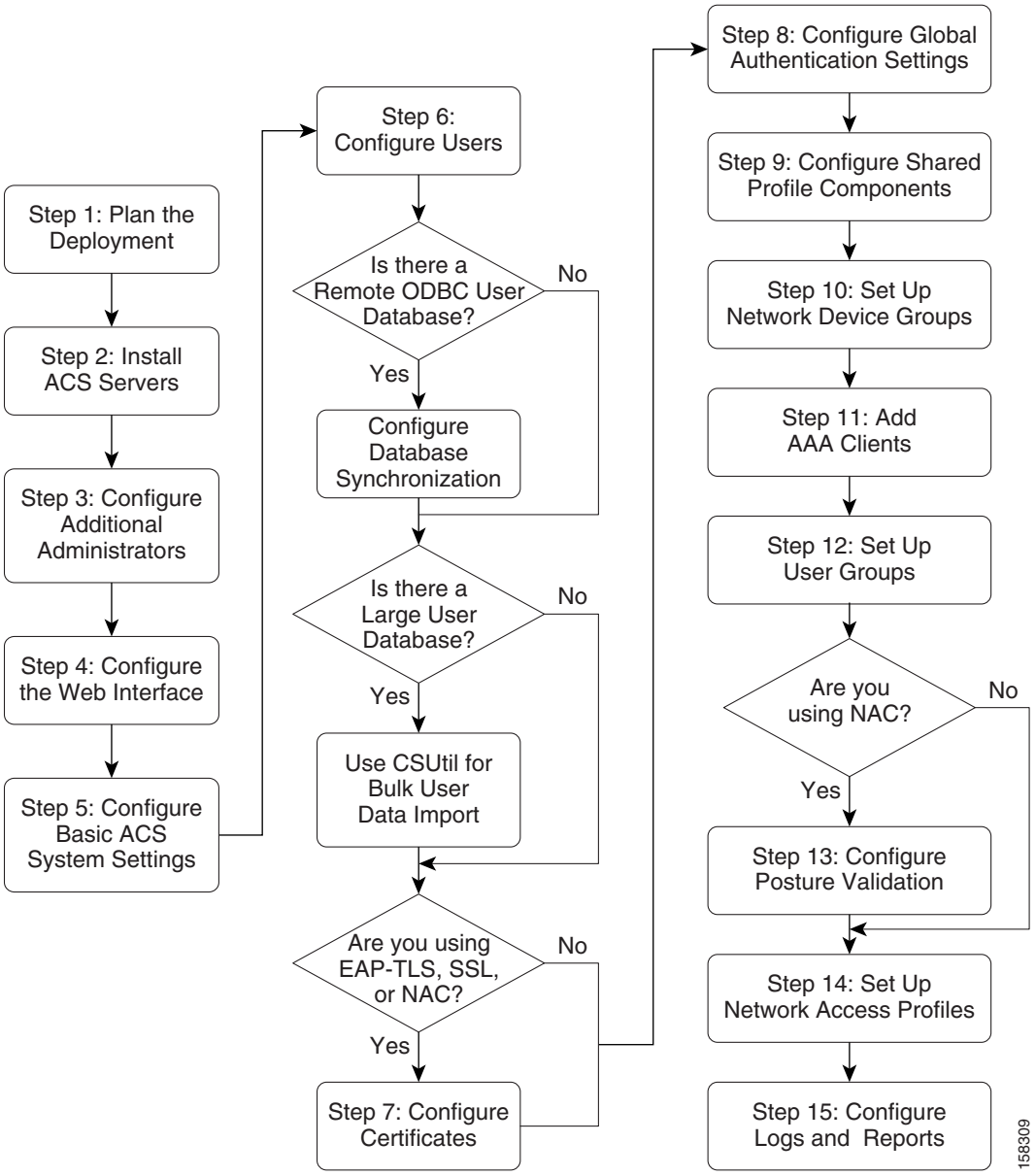
Step 15 Configure Logs and Reports.

Configure reports to specify how ACS logs data. You can also view the logs in HTML reports. For detailed instructions, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, "Logs and Reports.

Configuration Flowchart

Figure 1-1 is a configuration flowchart that shows the main steps in ACS configuration.

Figure 1-1 ACS Configuration Flowchart



Refer to the list of steps in Summary of Configuration Steps, page 1-1 for information on where to find detailed descriptions of each step.

CHAPTER 2

Deploy the Access Control Servers

This chapter discusses topics that you should consider before deploying Cisco Secure Access Control Server, hereafter referred to as ACS.

This document does not describe the software installation procedure for ACS or the hardware installation procedure for the ACS SE. For detailed installation information, refer to:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.2*, available on Cisco.com at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_windows/4.2/installation/guide/windows/IGwn42.html

- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*, available on Cisco.com at:

  http://www.cisco.com/en/US/docs/net_mgmt/cisco_secure_access_control_server_for_solution_engine/4.2/installation/guide/solution_engine/ACS_42_SE_install.html

Note For more detailed information on deploying ACS, see the *Cisco Secure Access Control Server Deployment Guide* at

http://www.cisco.com/application/pdf/en/us/guest/products/ps2086/c1244/cdccont_0900aecd80737943.pdf.

This chapter contains:

Determining the Deployment Architecture

How your enterprise network is configured and the network topology are likely to be the most important factors in deploying ACS.

This section discusses:

- **Access types**—How users will access the network (through wireless access, LAN access through switches, and so on) and the security protocols used to control user access; for example, RADIUS, EAP- TLS, Microsoft Active Directory, and so on.
- **Network architecture**—How the network is organized (centrally through campus LANs, regional LANs, WLANs, and so on.

This section contains:

Access Types

This section contains:

Wired LAN Access

You can use wired LAN access in a small LAN environment, a campus LAN environment, or a regionally or globally dispersed network. The number of users determines the size of the LAN or WLAN:

Size	Users
small LAN	1 to 3,000
medium-sized LAN	3,000 to 25,000
large LAN	25,000 to 50,000
very large LAN or WLAN	over 50,000

The wired LAN environment uses the following security protocols:

- **RADIUS**—RADIUS is used to control user access to wired LANs. In broadcast or switch-based Ethernet networks, you can use RADIUS to provide virtual LAN identification information for each authorized user.
- **EAP**—Extensible Authentication Protocol (EAP), provides the ability to deploy RADIUS into Ethernet network environments. EAP is defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards.

  The 802.1x standard, also known as EAP over LAN (EAPoL), concerns the part of the wider EAP standard that relates to broadcast media networks. Upon connection, EAPoL provides a communications channel between an end user on a client LAN device to the AAA server through the LAN switch. The functionality is similar to what Point-to-Point Protocol (PPP) servers on point-to-point links provide.

  By supporting complex challenge-response dialogues, EAP facilitates the user-based authentication demands of both conventional one-way hashed password authentication schemes such as Challenge Handshake Authentication Protocol (CHAP) and of more advanced authentication schemes such as Transport Layer Security (TLS), or digital certificates.

- **EAP-TLS**—Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). EAP-TLS uses the TLS protocol (RFC 2246), which is the latest version of the Secure Socket Layer (SSL) protocol from the IETF. TLS provides a way to use certificates for user and server authentication and for dynamic session key generation.
- **PEAP**— Protected Extensible Authentication Protocol (PEAP) is an 802.1x authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft that Cisco Systems, Microsoft, and RSA Security submitted to the IETF.

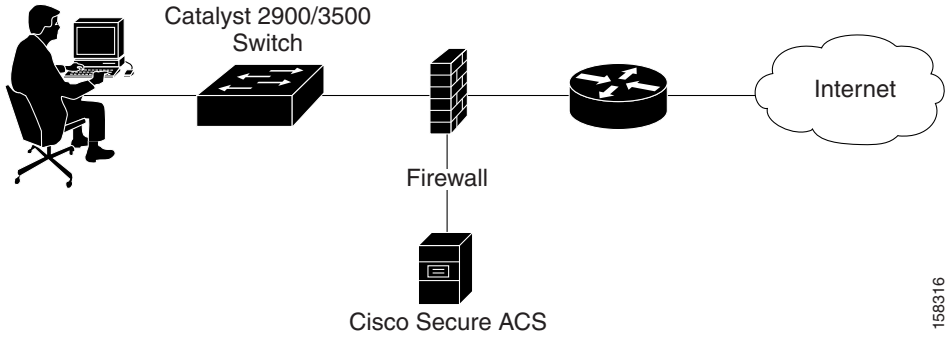
Small LAN Environment

In a small LAN environment (a LAN containing up to 3,000 users; see Figure 2-1), a single ACS is usually located close to the switch and behind a firewall. In this environment, the user database is usually small because few switches require access to ACS for AAA, and the workload is small enough to require only a single ACS.

However, you should still deploy a second ACS server for redundancy, and set up the second ACS server as a replication partner to the primary server; because, losing the ACS would prevent users from gaining access to the network. In Figure 2-1, an Internet connection via firewall and router are included because these are likely to be features of such a network; but, they are not strictly related to the Cisco Catalyst AAA setup or required as part of it.

You should also limit access to the system hosting the ACS to as small a number of users and devices as necessary. As shown in Figure 2-1, you set access by connecting the ACS host to a private LAN segment on the firewall. Access to this segment is limited only to the Cisco Catalyst Switch client and those user machines that require HTTP access to the ACS for administrative purposes. Users should not be aware that the ACS is part of the network.

Figure 2-1 ACS Server in a Small LAN Environment



Campus LAN

You can use ACS for wired access in a campus LAN. A campus LAN is typically divided into subnets. Figure 2-2 shows an ACS deployment in a wired campus LAN.

Figure 2-2 ACS in a Campus LAN

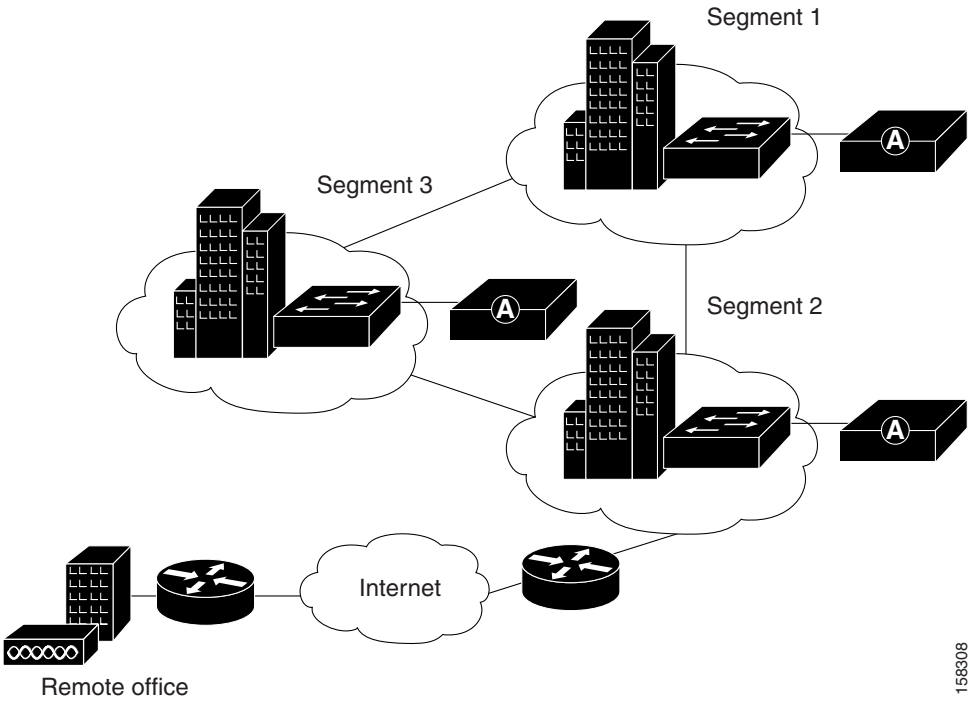


Figure 2-2 shows a possible distribution of ACS in a wired campus LAN. In this campus LAN, buildings are grouped into three segments. Each segment consists of 1 to 3 buildings and all the buildings in the segment are on a common LAN. All interbuilding and intersegment network connections use one-gigabyte fiber-optic technology. Primary network access is through switch ports over wired Ethernet.

You use ACS to provide RADIUS authentication for the network access servers, and you configure it to use an external database. One ACS is deployed for each segment of 5 to 10 buildings. A Cisco LocalDirector content switch is placed before each ACS for load balancing and failover.

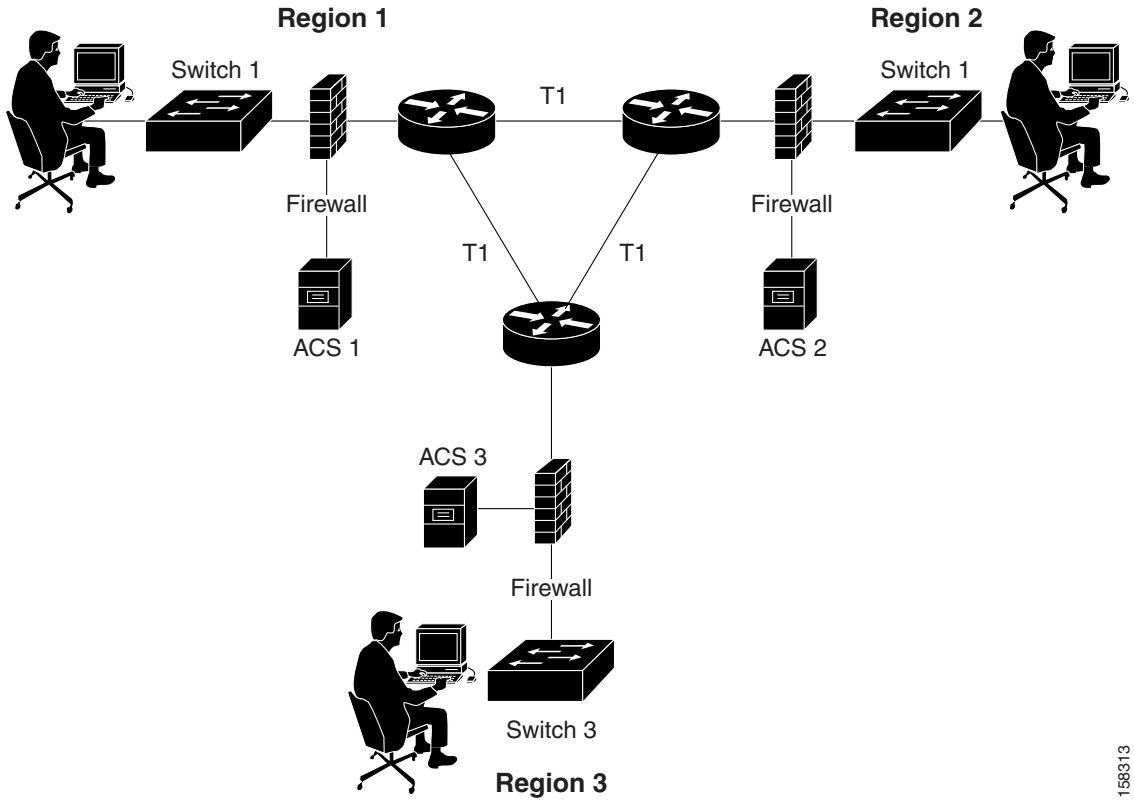
Geographically Dispersed Wired LAN

In a larger network that is geographically dispersed, speed, redundancy, and reliability are important in determining whether to use a centralized ACS service or a number of geographically dispersed ACS units. As with many applications, AAA clients rely on timely and accurate responses to their queries. Network speed is an important factor in deciding how to deploy ACS; because delays in authentication that the network causes can result in timeouts at the client side or the switch.

A useful approach in large extended networks, such as for a globally dispersed corporation, is to have at least one ACS deployed in each major geographical region. Depending on the quality of the WAN links, these servers may act as backup partners to servers in other regions to protect against failure of the ACS in any particular region.

Figure 2-3 shows ACS deployed in a geographically dispersed wired LAN. In the illustration, Switch 1 is configured with ACS 1 as its primary AAA server but with ACS 2 of Region 2 as its secondary. Switch 2 is configured with ACS 2 as its primary but with ACS 3 as its secondary. Likewise, Switch 3 uses ACS 3 as its primary but ACS 1 as its secondary. Using a local ACS as the primary AAA server minimizes AAA WAN traffic. When necessary, using the primary ACS from another region as the secondary further minimizes the number of ACS units.

Figure 2-3 ACS in a Geographically Dispersed LAN



Wireless Access Topology

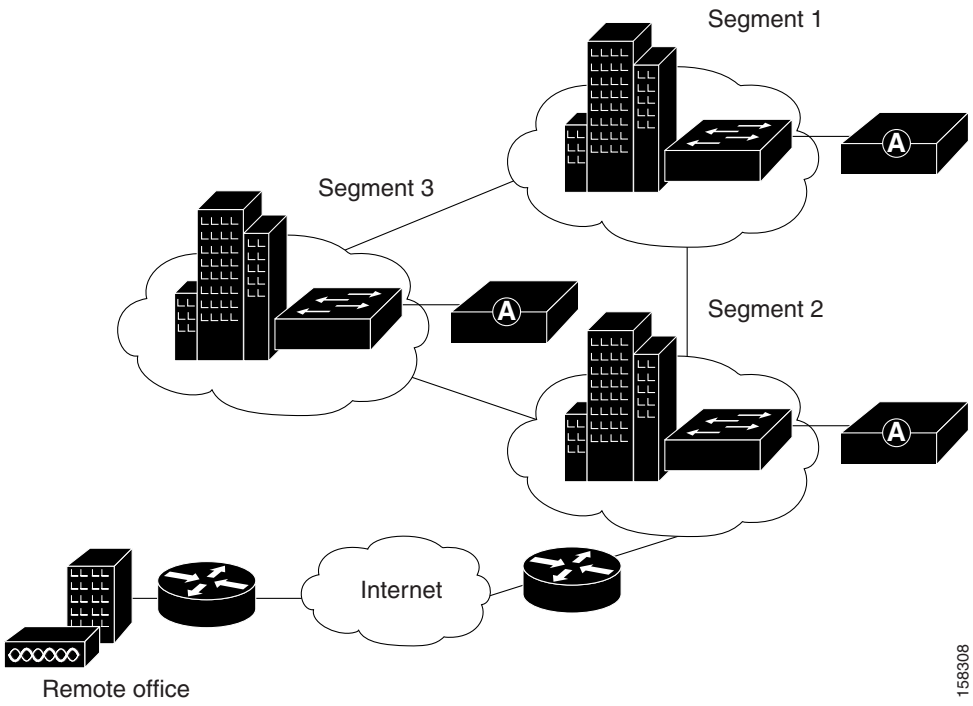
A wireless access point (AP), such as the Cisco Aironet series, provides a bridged connection for mobile end-user clients into the LAN. Authentication is absolutely necessary, due to the ease of access to the AP. Encryption is also necessary because of the ease of eavesdropping on communications.

Scaling can be a serious issue in the wireless network. The mobility factor of the WLAN requires considerations similar to those given to the dial-up network. Unlike the wired LAN, however, you can more readily expand the WLAN. Though WLAN technology does have physical limits as to the number of users who can connect via an AP, the number of APs can grow quickly. As with the dial-up network, you can structure your WLAN to allow full access for all users, or provide restricted access to different subnets among sites, buildings, floors, or rooms. This capability raises a unique issue with the WLAN: the ability of a user to roam among APs.

Simple WLAN

A single AP might be installed in a simple WLAN (Figure 2-4). Because only one AP is present, the primary issue is security. An environment such as this generally contains a small user base and few network devices. Providing AAA services to the other devices on the network does not cause any significant additional load on the ACS.

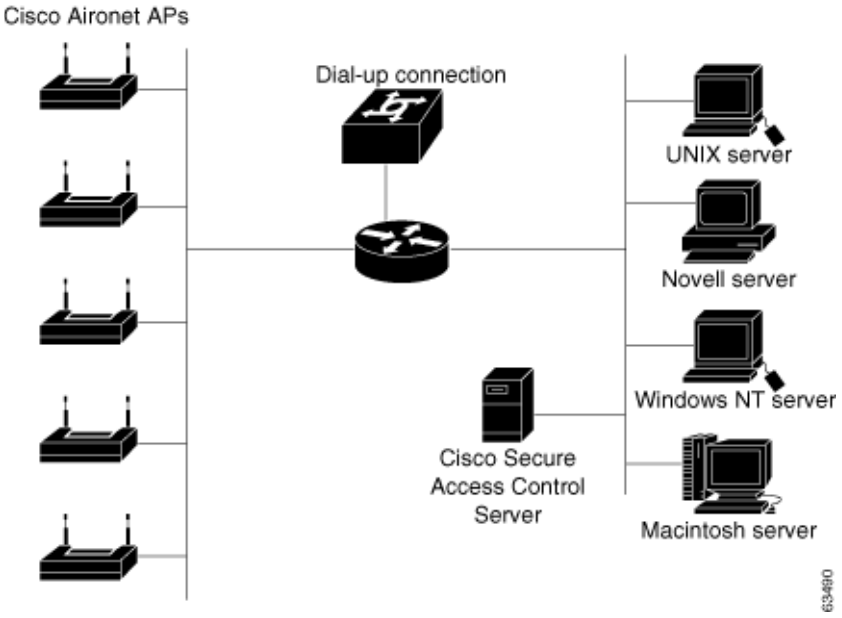
Figure 2-4 Simple WLAN



Campus WLAN

In a WLAN where a number of APs are deployed, as in a large building or a campus environment, your decisions on how to deploy ACS become more complex. Depending on the processing needs of the installation, all of the APs might be on the same LAN. Figure 2-5 shows all APs on the same LAN; however, the APs might also be distributed throughout the LAN, and connected via routers, switches, and so on.

Figure 2-5 Campus WLAN

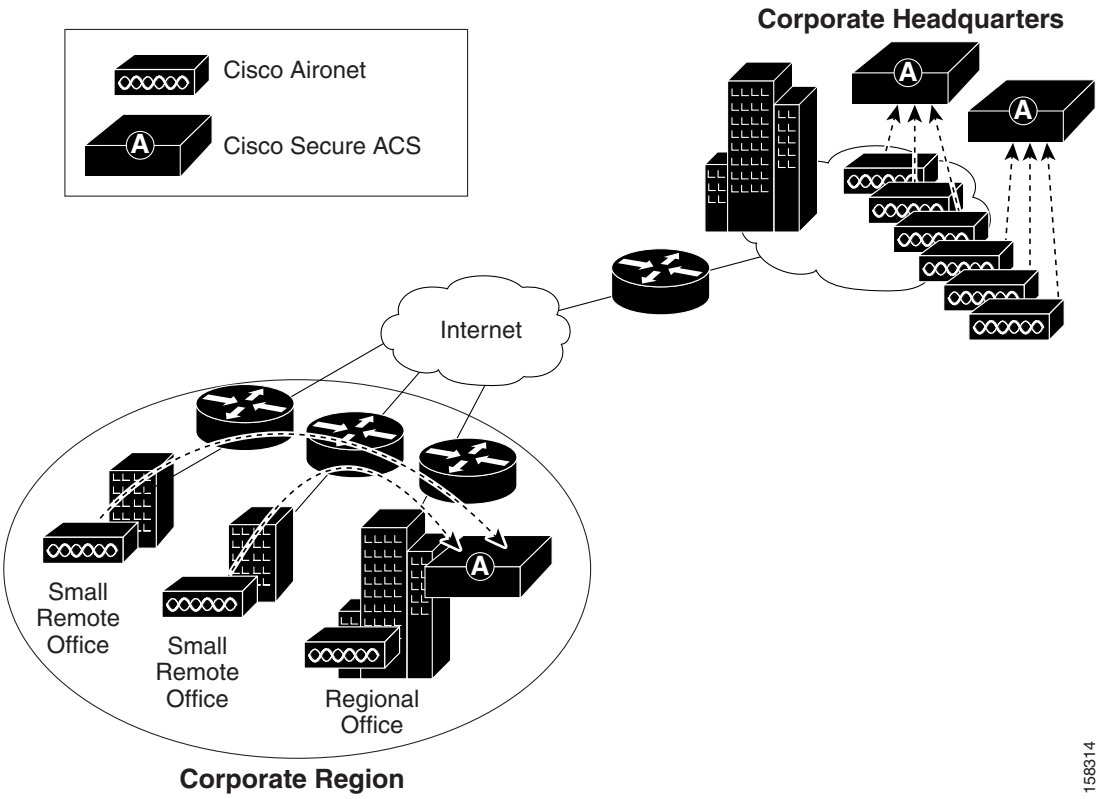


Regional WLAN Setting

In a given geographical or organizational region, the total number of users might or might not reach a critical level for a single ACS. Small offices would not qualify for separate installations of ACSs and a regional office might have sufficient reserve capacity. In this case, the small offices can authenticate users across the WAN to the larger regional office. Once again, you should determine that this does not pose a risk to the users in the remote offices. Assess critical connectivity needs against the reliability and throughput to the central ACS.

Figure 2-6 shows a regional WLAN.

Figure 2-6 ACS in a Regional WLAN



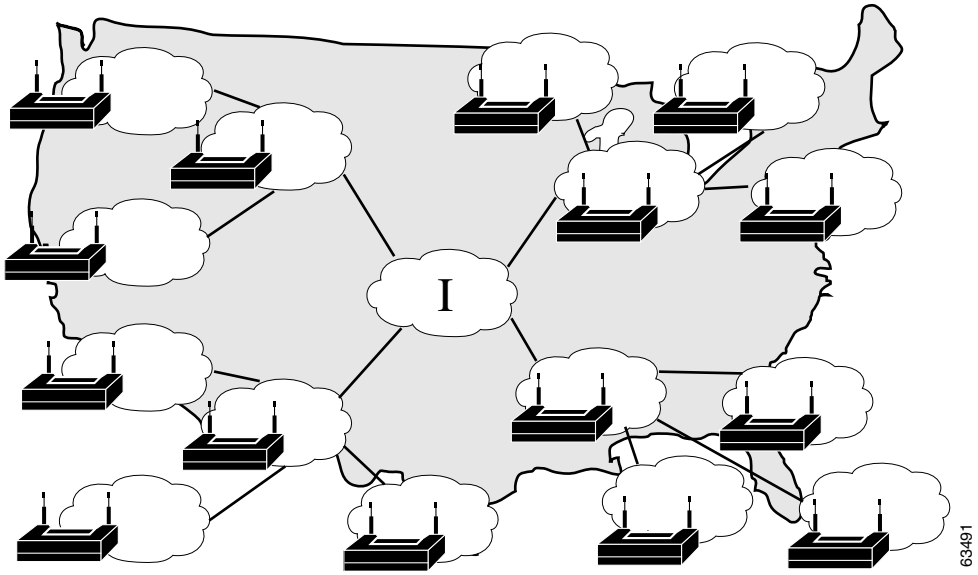
Large Enterprise WLAN Setting

In a very large geographically dispersed network (over 50,000 users), access servers might be located in different parts of a city, in different cities, or on different continents. If network latency is not an issue, a central ACS might work; but, connection reliability over long distances might cause problems. In this case, local ACSs may be preferable to a central ACS.

If the need for a globally coherent user database is most important, database replication or synchronization from a central ACS may be necessary. For information on database replication considerations, see Database Replication Considerations, page 2-13 and Database Synchronization Considerations, page 2-14. Authentication by using external databases, such as a Windows user database or the Lightweight Directory Access Protocol (LDAP), can further complicate the deployment of distributed, localized ACSs.

Figure 2-7 shows ACS installations in a geographically dispersed network that contains many WLANs.

Figure 2-7 ACS in a Geographically Dispersed WLAN



For the model in Figure 2-7, the location of ACS depends on whether all users need access on any AP, or require only regional or local network access. Along with database type, these factors control whether local or regional ACSs are required, and how database continuity is maintained. In this very large deployment model (over 50,000 users), security becomes a more complicated issue, too.

Additional Considerations for Deploying ACS in a WLAN Environment

You should also consider the following when deploying ACS in a WLAN environment, consider if:

- Wireless is secondary to wired access, using a remote ACS as a secondary system is acceptable.
- Wireless is the primary means of access, put a primary ACS in each LAN.
- The customer uses ACS for user configuration, data replication is critical.

Dial-up Access Topology

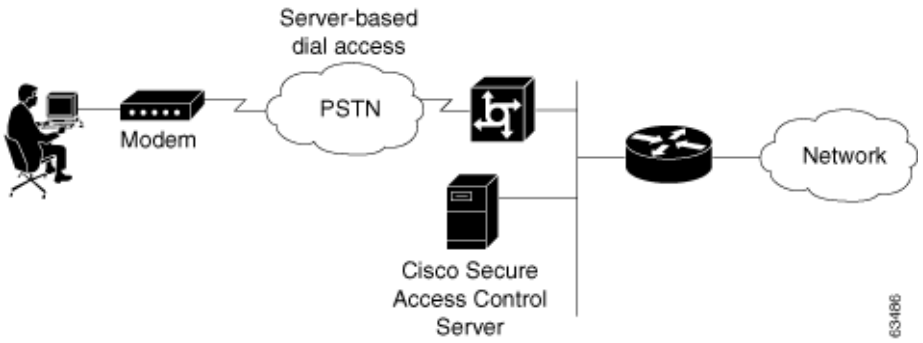
Until recently, dial-up access was the most prevalent method for providing remote access to network resources. However, DSL access and access through VPNs have largely replaced dial-up access through modems.

ACS is still used in some LAN environments to provide security for dial-up access. You can provide dial-up access for a small LAN or for a large dial-in LAN.

Small Dial-Up Network Access

In the small LAN environment, see Figure 2-8, network architects typically place a single ACS internal to the AAA client, which a firewall and the AAA client protect from outside access. In this environment, the user database is usually small; because, few devices require access to the ACS for authentication, authorization and accounting (AAA), and any database replication is limited to a secondary ACS as a backup.

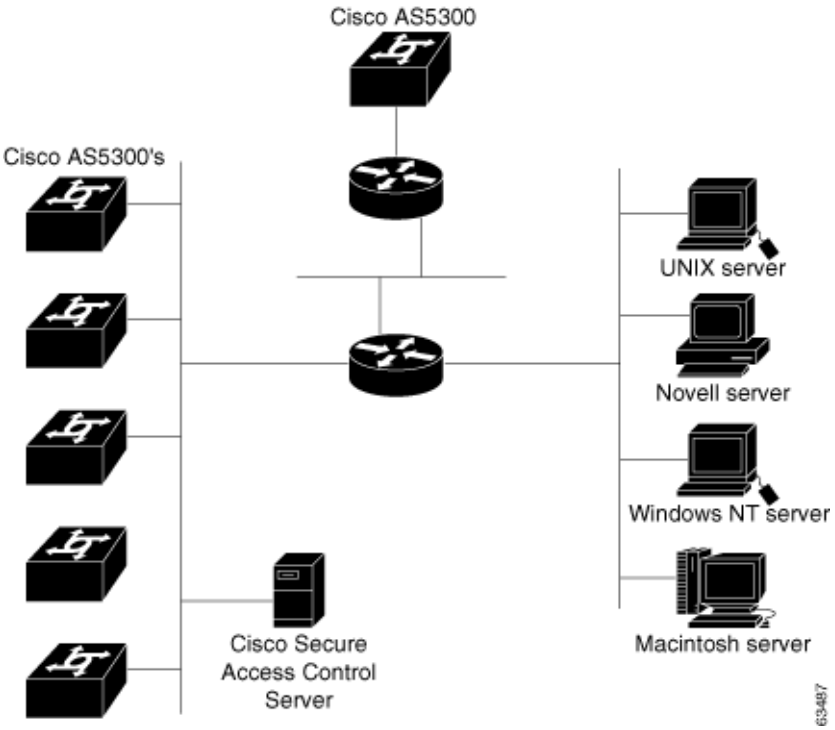
Figure 2-8 Small Dial-up Network



Large Dial-Up Network Access

In a larger dial-in environment, a single ACS with a backup may be suitable, too. The suitability of this configuration depends on network and server access latency. Figure 2-9 shows an example of a large dial-in network. In this scenario, the addition of a backup ACS is recommended.

Figure 2-9 Large Dial-up Network



Placement of the RADIUS Server

From a practical standpoint, the RADIUS server should be inside the general network, preferably within a secure subnet designated for servers, such as DHCP, Domain Name System (DNS), and so on. You should avoid requiring RADIUS requests to travel over WAN connections because of possible network delays and loss of connectivity. Due to various reasons, this type of configuration is not always possible; for example, with small remote subnets that require authentication support from the enterprise.

You must also consider backup authentication. You may use a system that is dedicated as the RADIUS secondary. Or, you may have two synchronized systems that each support a different network segment but provide mutual backup if one fails. Refer to the documentation for your RADIUS server for information on database replication and the use of external databases.

Determining How Many ACSs to Deploy (Scalability)

A number of factors affect the scalability of an ACS installation (that is, how effectively each ACS can process user access requests) and how many ACS servers you should deploy in the network.

For detailed information on scalability considerations, see the following white papers on ACS deployment, which are available on Cisco.com at:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html

- *Building a Scalable TACACS+ Device Management Framework*
- *Catalyst Switching and ACS Deployment Guide*
- *Deploying Cisco Secure ACS for Windows in Cisco Aironet Environment*
- *EAP-TLS Deployment Guide for Wireless LAN Networks*
- *Guidelines for Placing ACS in the Network*

This section contains:

Number of Users

In all topologies, the number of users is an important consideration. For example, assuming that an ACS can support 21,000 users, if an wireless access point can support 10 users, then a given ACS could support 2,100 wireless access points in a WLAN environment.

The size of the LAN or WLAN is determined by the number of users who use the LAN or WLAN:

Size	Users
Small LAN	1 to 3,000
Medium-sized LAN	3,000 to 25,000
Large LAN	25,000 to 50,000
Very large LAN or WLAN	Over 50,000

For a detailed formula, see the white paper *Deploying Cisco Secure ACS for Windows in Cisco Aironet Environment*, which is available on Cisco.com at this location:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html

Number of Network Access Servers

An ACS can support up 5,000 discrete network access servers (NASs). You can use the multi-NAS capability of ACS to increase this number.

LAN Versus WAN Deployment (Number of LANs in the Network)

In general, you should provide one ACS server per LAN. If a backup ACS is required, the backup ACS may reside on the same LAN or can be an ACS on another LAN.

WAN Latency and Dependability

The distance between LANs in a large network (25,000 to 50,000 users) is also a consideration.

If the network is centralized, one primary ACS and one secondary ACS might be sufficient.

If the network is geographically dispersed, the number of ACS servers required varies with the needs of the regions. For example:

- Some regions may not need a dedicated ACS.
- Larger regions (regions with over 10,000 users), such as corporate headquarters, might need several ACSs.

The distance between subnets is also a consideration. If subnets are close together, the connections will be more reliable, and fewer ACS servers will be needed. Adjacent subnets could serve other buildings with reliable connections. If the subnets are farther apart, more ACS servers might be needed.

The number of subnets and the number of users on each subnet is also a factor. For example, in a WLAN, a building may have 400 potential users and the same subnet might comprise four buildings. One ACS assigned to this subnet will service 1,600 users (about one tenth of the number of current users). Other buildings could be on adjacent subnets with reliable WAN connections. ACSs on adjacent subnets could then be used as secondary systems for backup.

If the WAN connections between buildings in this subnet are short, reliable, and pose no issue of network latency, two ACSs can service all of these buildings and all the users. At 40-percent load, one ACS would take half of the access points as the primary server, and the other ACS would take the remaining APs. Each ACS would provide backup for the other. Again, at 40-percent load, a failure of one ACS would

only create an 80-percent load on the other ACS for the duration of the outage. If the WAN is not suitable for authentication connections, we recommend using two or more ACSs on the LAN in a primary or secondary mode or load balanced.

Determining How Many ACS Servers to Deploy in Wireless Networks

In planning how many ACS servers to deploy in a wireless network, consider:

- The location and number of access points. For example, with 4,200 APs:
  - One ACS could handle half of the APs as primary server.
  - Other ACSs could handle the remaining APs.
- The number of EAP-TLS clients together with EAP-TLS authentications per second
- The number of clients
- Scalability with different protocols

  For example, if you use EAP-TLS, you will need more ACS servers; but, if you use PEAP, you will need fewer. EAP-TLS is slower than PEAP due to public-key infrastructure (PKI) processing time.

For a detailed formula that you can be use to calculate the number of ACS servers required in a wireless network, see the white paper titled *Deploying Cisco Secure ACS for Windows in an Aironet Environment*, available on Cisco.com at:

http://www.cisco.com/en/US/products/sw/secursw/ps2086/prod_white_papers_list.html

Deploying ACS Servers to Support Server Failover

This section discusses deployment topologies for implementing server failover. This section contains:

Load Balancing and Failover

To implement load balancing, you can set up user groups and then assign groups to a specific RADIUS server (usually the nearest RADIUS server).

Database Replication Considerations

Database replication replicates selected database information, such as user and group information, from a primary ACS to one or more ACS backups or clients. The following aspects of replication are configurable with ACS:

- **Configuration components for replication**—What is replicated.
- **Replication scheduling**—When replication occurs.
- **Replication frequency**—How often systems are replicated.
- **Replication partners**—Which systems are replicated.

- **Client configuration**—How to configure the client.
- **Reports and event (error) handling**—What information to include in the logs.

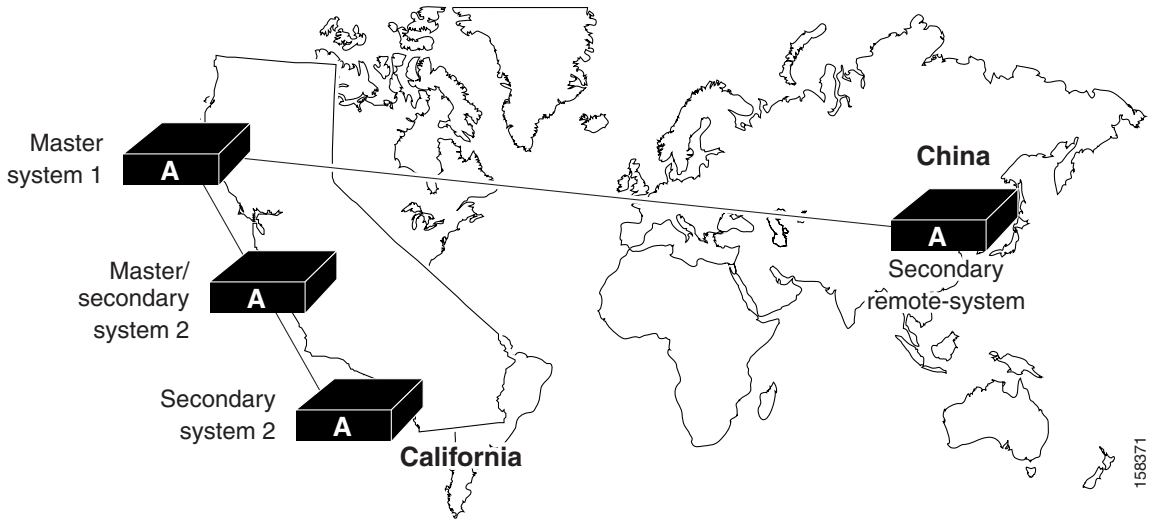
Replication Design

Because database replication in a ACS is a top-down approach, using the cascade method minimizes replication-induced downtime on the master server. If the primary server is not used for authentication services, but for database maintenance only, the cascade method may not be as critical.

However, when traveling across time zones, particularly international time zones, it may be necessary to use the cascade method going to remote secondaries. In this case, when you configure database replication on the Database replication setup page, click At specific times instead of Automatically triggered cascade.

Use the automatically triggered cascade method so that local replication occurs during a time that will minimize the impact on user authentication. During these long-distance replications, replicating to the backup or secondary server first also helps reduce this impact. Figure 2-10 shows a hypothetical deployment for replication where each region has a primary and a secondary ACS deployed. In this scenario, replication is made to the secondary servers to avoid replication downtime to the primary, but, may not be needed if the primary is used mainly for database maintenance but not for authentication.

Figure 2-10 ACS Database Replication Scenario



Database Synchronization Considerations

An alternative to database replication is the use of Relational Database Management System (RDBMS) synchronization. You use the RDBMS synchronization feature to update the ACS user database with information from an Open Database Connectivity (ODBC)-compliant data source. The ODBC-compliant data source can be the RDBMS database of a third-party application. It can also be an intermediate file or database that a third-party system updates. Regardless of where the file or database resides, ACS reads the file or database via the ODBC connection. RDBMS synchronization supports addition, modification, and deletion for all data items it can access.

Deploying ACS in a NAC/NAP Environment

You can deploy ACS in a Cisco Network Admission Control and Microsoft Network Access Protection (NAC/NAP) environment. In the NAC/NAP environment, NAP client computers authorize with ACS by using EAP over UDP (EoU) or EAP over 802.1x.

Table 2-1 describes the components of a NAC/NAP deployment.

Table 2-1 Components of a NAC/NAP Deployment

Component	Description
NAP client	A computer running Windows Vista or Windows Server 2008. NAP clients send their health credentials as Statements of Health (SoHs) or as a health certificate.
NAP agent	A process running on a NAP client that sends SoHs or health certificates to ACS.
Network access devices	Cisco devices through which you can access the network, such as routers, switches, wireless access points, and VPN concentrators.
ACS	Cisco AAA server product.
Network Policy Server (NPS)	A Microsoft server that validates health certificates from NAP clients and provides remediation instructions if needed.
Health Registration Authority	A Microsoft certificate server that obtains health certificates on behalf of NAP clients from a public key infrastructure (PKI).
Policy Servers	Servers that provide current system health state for Microsoft NPSs.

When a NAP client connects, it uses a NAP agent to send ACS one of the following:

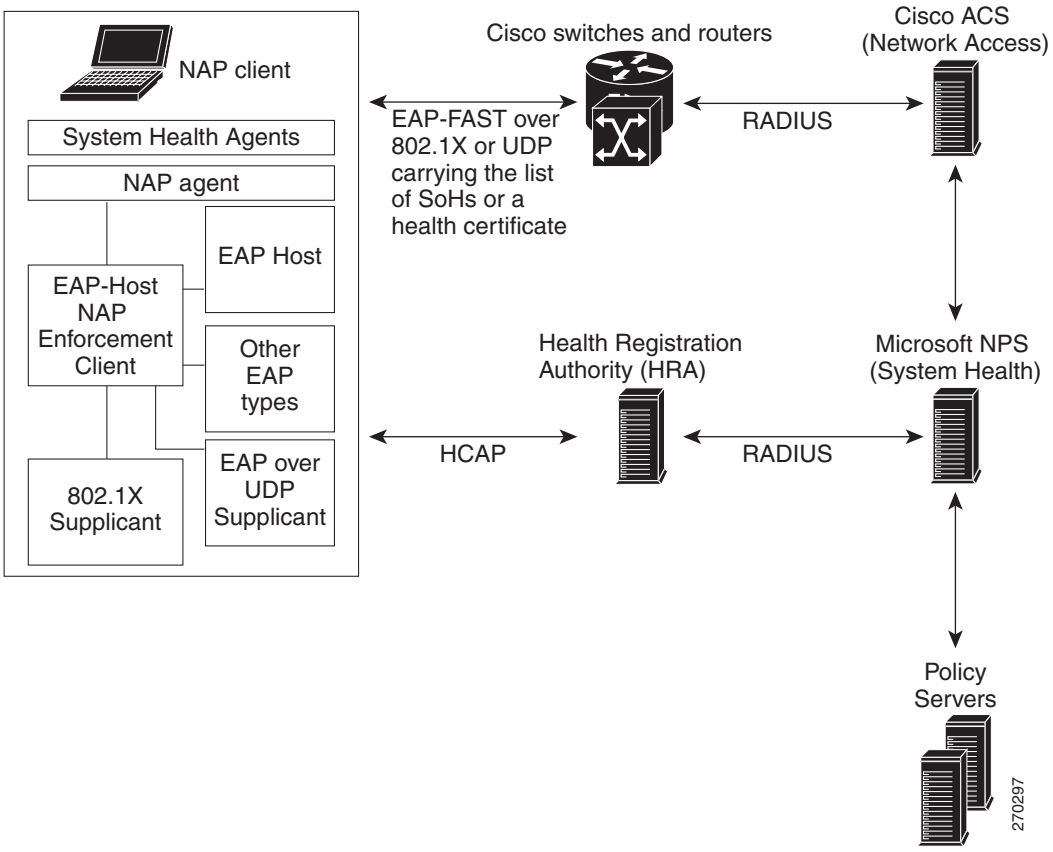
- A list of SoHs.
- A certificate that the client has received from a Microsoft Health Registration Authority (HRA).

The ACS host validates the client credentials. If the NAP agent sends a:

- List of SoHs, the ACS sends the list to a Microsoft NPS by using the Cisco Host Credentials Authorization Protocol (HCAP). The NPS evaluates the SoHs. The ACS then sends an appropriate NAP to the network access device (switch, router, VPN, and so on) to grant the authorized level of access to the client.
- Health certificate rather than a list of SoHs, then ACS validates the certificate as the EAP-FAST session is established to determine the overall health of the client. The ACS then sends the appropriate NAP to the network to grant the authorized level of access to the client.

Figure 2-11 illustrates the architecture of a NAC/NAP network.

Figure 2-11 NAC/NAP Deployment Architecture



Additional Topics

This section describes additional topics to consider when deploying ACS. This section contains:

Remote Access Policy

Remote access is a broad concept. In general, it defines how the user can connect to the LAN, or from the LAN to outside resources (that is, the Internet). Connectivity is possible in many ways: dial-in, ISDN, wireless bridges, and secure Internet connections. Each method incurs its own advantages and disadvantages, and provides a unique challenge to providing AAA services. In addition to the method of

access, other decisions can also affect how ACS is deployed; these include specific network routing (access lists), time-of-day access, individual restrictions on AAA client access, access control lists (ACLs), and so on.

You can implement remote-access policies for employees who telecommute, or mobile users who dial in over ISDN or a public switched telephone network (PSTN). Such policies are enforced at the corporate campus with ACS and the AAA client. Inside the enterprise network, remote-access policies can control wireless access by individual employees.

ACS remote-access policies provide control by using central authentication and authorization of remote users. The Cisco user database maintains all user IDs, passwords, and privileges. You can download ACS policies in the form of ACLs to network access servers such as the Cisco AS5300 Network Access Server, or by allowing access during specific periods, or on specific access servers.

Remote-access policies are part of the overall Cisco corporate security policy.

Security Policy

Every organization that maintains a network should develop a security policy for the organization. The sophistication, nature, and scope of your security policy directly affect how you deploy ACS.

For more information about developing and maintaining a comprehensive security policy, refer to these documents:

- Network Security Policy: Best Practices White Paper
- Cisco IOS Security Configuration Guide

Administrative Access Policy

Managing a network is a matter of scale. Providing a policy for administrative access to network devices depends directly on the size of the network and the number of administrators required to maintain the network. A network device can be authenticated locally; but, this ability is not scalable. The use of network management tools can help in large networks (25,000 to 50,000 users); but, if local authentication is used on each network device, the policy usually entails a single login on the network device. A single login on the network device does not provide adequate network device security.

ACS provides a centralized administrator database, and you can add or delete administrators at one location. TACACS+ is the recommended AAA protocol for controlling AAA client administrative access because of its ability to provide per-command control (command authorization) of AAA client administrator access to the device. RADIUS is not well suited for this purpose because of the one-time transfer of authorization information at the time of initial authentication.

The type of access is also an important consideration. In the case of different administrative access levels to the AAA clients, or if a subset of administrators is to be limited to certain systems, you can use ACS with command authorization per network device to restrict network administrators as necessary. Using local authentication restricts the administrative access policy to no login on a device or by using privilege levels to control access.

Controlling access by means of privilege levels is cumbersome and not very scalable. Such control requires altering the privilege levels of specific commands on the AAA client device and defining specific privilege levels for the user login. You can easily create more problems by editing command privilege levels. Using command authorization on ACS does not require that you alter the privilege level of controlled commands. The AAA client sends the command to ACS to be parsed and ACS determines whether the administrator has permission to use the command. The use of AAA allows authentication on any AAA client for any user on ACS and limits access to these devices on a per-AAA-client basis.

A small network with a small number of network devices may require only one or two individuals to administer it. Local authentication on the device is usually sufficient. If you require more granular control than what authentication can provide, some means of authorization is necessary. As discussed earlier, controlling access by using privilege levels can be cumbersome. ACS reduces this problem.

In large enterprise networks, with many devices to administer, the use of ACS practically becomes a necessity. Because administration of many devices requires a larger number of network administrators, with varying levels of access, the use of local control is simply not a viable way to track network-device configuration changes that are required when changing administrators or devices.

The use of network management tools, such as CiscoWorks, helps to ease this burden; but, maintaining security is still an issue. Because ACS can comfortably handle up to 300,000 users, the number of network administrators that ACS supports is rarely an issue. If a large remote-access population is using RADIUS for AAA support, the corporate IT team should consider separate TACACS+ authentication by using ACS for the administrative team. Separate TACACS+ authentication would isolate the general user population from the administrative team and reduce the likelihood of inadvertent access to network devices. If the use of TACACS+ is not a suitable solution, using TACACS+ for administrative (shell or exec) logins, and RADIUS for remote network access, provides sufficient security for the network devices.

Separation of Administrative and General Users

You should prevent the general network user from accessing network devices. Even though the general user may not intend to gain unauthorized access, inadvertent access could accidentally disrupt network access. AAA and ACS provide the means to separate the general user from the administrative user.

The easiest and recommended method to perform such separation is to use RADIUS for the general remote-access user and TACACS+ for the administrative user. One issue is that an administrator may also require remote network access, like the general user. If you use ACS, this issue poses no problem. The administrator can have RADIUS and TACACS+ configurations in ACS. By using authorization, RADIUS users can set PPP (or other network access protocols) as the permitted protocol. Under TACACS+, only the administrator would be configured to have shell (exec) access.

For example, if the administrator is dialing in to the network as a general user, a AAA client would use RADIUS as the authenticating and authorizing protocol, and the PPP protocol would be authorized. In turn, if the same administrator remotely connects to a AAA client to make configuration changes, the AAA client would use the TACACS+ protocol for authentication and authorization. Because this administrator is configured on ACS with permission for shell under TACACS+, the administrator would be authorized to log in to that device. This does require that the AAA client have two separate configurations on ACS, one for RADIUS and one for TACACS+.

An example of a AAA client configuration under IOS that effectively separates PPP and shell logins is:

```
aaa new-model
tacacs-server host ip-address
tacacs-server key secret-key
radius-server host ip-address
radius-server key secret-key
aaa authentication ppp default group radius
aaa authentication login default group tacacs+ local
aaa authentication login console none
aaa authorization network default group radius
aaa authorization exec default group tacacs+ none
aaa authorization command 15 default group tacacs+ none
username user password password
line con 0
login authentication console
```

Conversely, if a general user attempts to use his or her remote access to log in to a network device, ACS checks and approves the username and password; but, the authorization process would fail because that user would not have credentials that allow shell or exec access to the device.

Database Considerations

Aside from topological considerations, the user database is one of the most influential factors in deployment decisions for ACS. The size of the user base, distribution of users throughout the network, access requirements, and type of user database are all factors to consider when you decide how to deploy ACS.

Number of Users

ACS is designed for the enterprise environment, and can handle 300,000 users. This capacity is usually more than adequate for a corporation. In an environment that exceeds these numbers, the user base would typically be geographically dispersed, which requires the use of more than one ACS configuration. A WAN failure could render a local network inaccessible because of the loss of the authentication server. In addition, reducing the number of users that a single ACS handles improves performance by lowering the number of logins occurring at any given time and reducing the load on the database.

Type of Database

ACS supports several database options, including the ACS internal database or by using remote authentication with any of the external databases that ACS supports. Each database option has its own advantages and limitations in scalability and performance.

Network Latency and Reliability

Network latency and reliability are also important factors in how you deploy ACS. Delays in authentication can result in timeouts for the end-user client or the AAA client.

The general rule for large, extended networks, such as those in a globally dispersed corporation, is to have at least one ACS deployed in each region. This configuration may not be adequate without a reliable, high-speed connection between sites. Many corporations use secure VPN connections between sites so that the Internet provides the link. Although this option saves time and money, it does not provide the speed and reliability of a dedicated frame relay or T1 link. If a reliable authentication service is critical to business functionality, such as a WLAN of retail outlets with cash registers that are linked by a WLAN, the loss of WAN connection to a remote ACS could be catastrophic.

The same issue can be applied to an external database that ACS uses. You should deploy the database close enough to ACS to ensure reliable and timely access. Using a local ACS with a remote database can result in the same problems as using a remote ACS. Another possible problem in this scenario is that a user may experience timeout problems. The AAA client would be able to contact ACS; but, ACS would wait for a reply that might be delayed or never arrive from the external user database. If the ACS were remote, the AAA client would time out and try an alternate method to authenticate the user; but, in the latter case, it is likely the end-user client would time out first.

CHAPTER 3

Configuring New Features in ACS 4.2

This chapter describes how to configure several new features provided with ACS 4.2.

For information on new features that accompany both ACS for Windows and the ACS SE, see:

For information on new features that accompany ACS SE only, see:

New Global EAP-FAST Configuration Options

The EAP-FAST Configuration page in the Global Authentication Setup section contains several new options. Figure 3-1 shows the new options on the EAP-FAST Configuration page.

Figure 3-1 New Global EAP-FAST Configuration Options

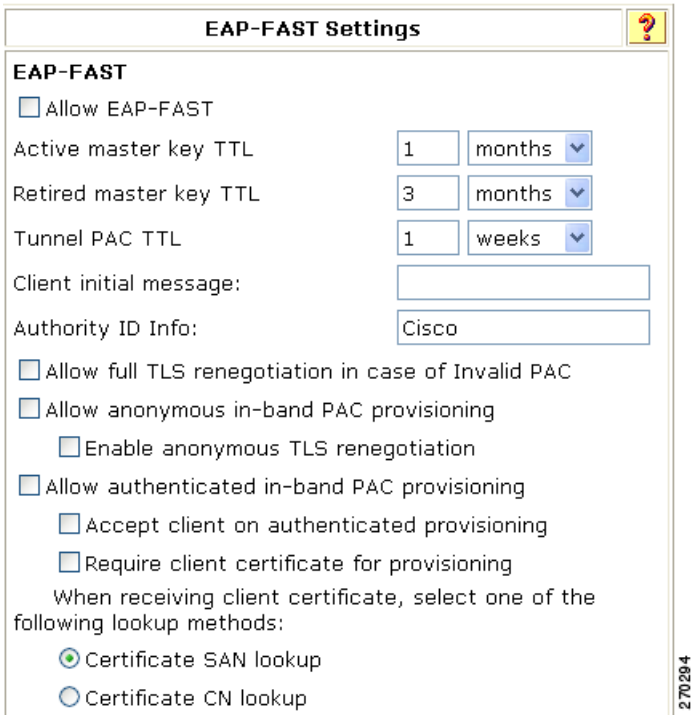


Table 3-1 describes the new EAP-FAST settings.

Table 3-1 New EAP-FAST Global Configuration Settings with Release 4.2

Option	Description
Allow Full TLS Renegotiation in Case of Invalid PAC	This option handles cases of an invalid or expired PAC. In this situation, the EAP server can select a different cipher than the one normally used with the invalid PAC to start the full TLS handshake and authentication. Check the Allow Full TLS Renegotiation in Case of Invalid PAC check box if you have clients that might attempt to authenticate by using certificates that are unusually old.
Allow Anonymous In-band PAC Provisioning	ACS provisions an end-user client with a PAC using EAP-FAST phase zero. If you check this check box, ACS establishes a secured connection with the end-user client to provide the client with a new PAC.
Enable anonymous TLS renegotiation	If you check the Allow Anonymous in-band PAC Provisioning check box, you can also check the Enable anonymous TLS renegotiation check box. Check the Enable anonymous TLS renegotiation check box if your network contains Vista clients, to prevent Vista users from being prompted twice for their password.

Disabling of EAP-FAST PAC Processing in Network Access Profiles

In the Protocols section for Network Access Profile (NAP) configuration, you can now set up a NAP that causes ACS to use EAP-FAST but not issue or accept tunnel or machine PACs.

Figure 3-2 shows the EAP-FAST section of the NAP Protocols page for ACS 4.2.

Figure 3-2 Use PAC and Do Not Use PAC Options

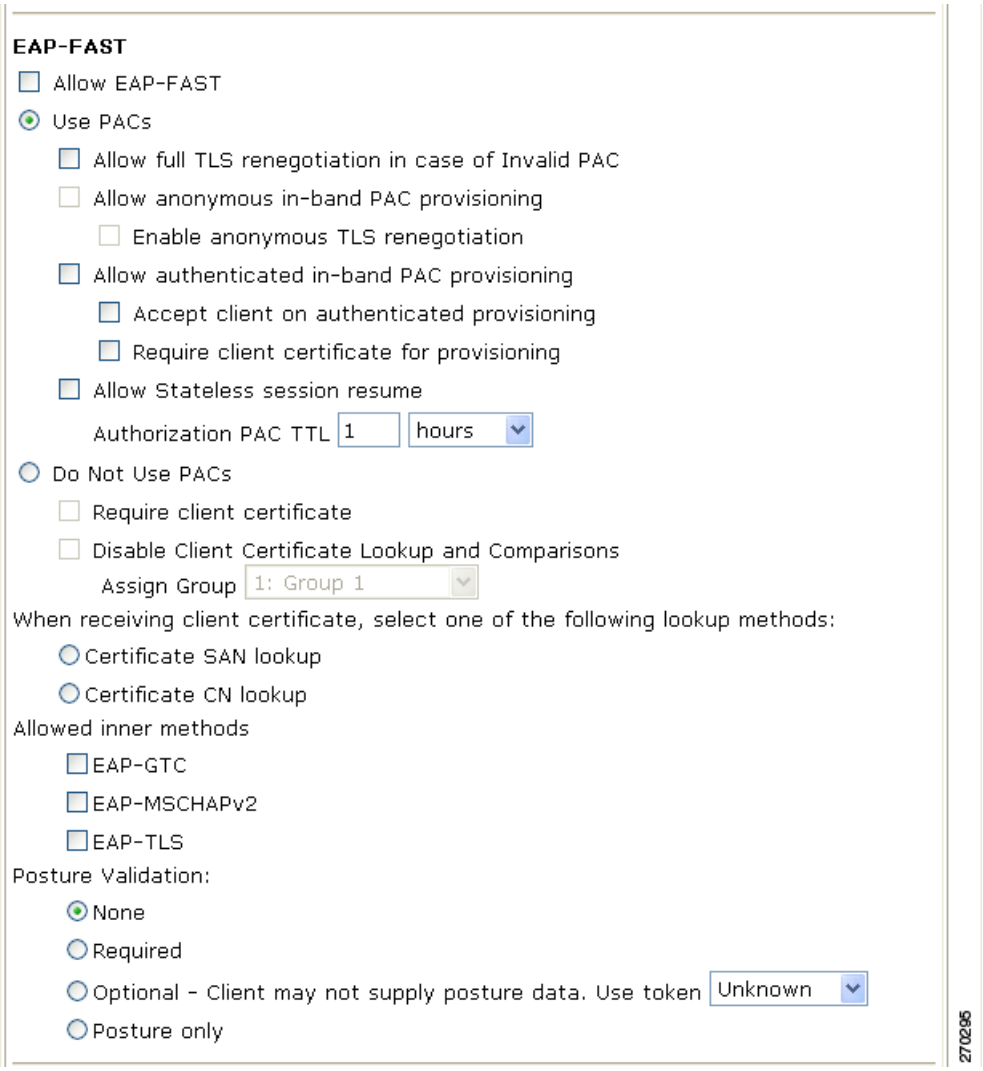


Figure 3-2 shows the new options on the NAP Protocols page.

Table 3-2 New Options on the NAP Protocols Page

Option	Description:
Use PACs	Click the Use PACs radio button if you want ACS to authenticate clients to which this NAP is applied by using EAP-FAST with PACs enabled. If you click the Use PACs radio button, then the same EAP-FAST configuration options that are available in the global EAP-FAST configuration are available.
Do Not Use PACs	Click the Do Not Use PACs radio button if you want ACS to authenticate clients to which this NAP is applied by using EAP-FAST without PACs enabled.
Require Client Certificate	If you click the Do Not Use PACs radio button, the Require Client Certificate option is available. Choose this option to require a client certification for EAP-FAST tunnel establishment.
Disable Client Certificate Lookup and Comparisons	If you click the Do Not Use PACs radio button, you can check the Disable Client Certificate Lookup and Comparisons check box to disable client certificate lookup and to enable EAP-FAST PKI Authorization Bypass. If you check the Disable Client Certificate Lookup and Comparisons check box, ACS establishes an EAP-FAST tunnel without authorizing the user based on user group data or a public key infrastructure (PKI) certificate in a user database; instead, ACS maps the user to a preconfigured user group.
Assign Group	If you check the Disable Client Certificate Lookup and Comparisons check box; then, from the drop-down list of user groups in the Assign Group field, select a user group to apply to the client.

Disabling NetBIOS

Because disabling NetBIOS might be desirable in some cases, you can run ACS 4.2 with NetBIOS disabled.

ACS SE 4.2 runs on a customized version of Windows 2003 that includes some but not all Windows 2003 services.

Note Although you can use Windows 2000, Windows XP, and Windows Server 2003 to disable NetBIOS over TCP/IP (NetBT), many corporate networks do not, since most of them still have legacy (Windows 9.x or Windows NT) machines on their network. These machines need NetBIOS to function properly on a network, since they use NetBIOS to log in to domains, find one another, and establish sessions for accessing shared resources.

To disable NetBIOS over TCP/ IP in Windows 2000, XP, or 2003:

Step 1 Right-click **My Network Places** and choose **Properties**.

Step 2 Right-click the appropriate Local Area Connection icon, and click **Properties**.

Step 3 Click **Internet Protocol (TCP/IP)** and choose **Properties**.

Step 4 Click **Advanced**, and click the **WINS** tab.

Step 5 On the WINS tab, enable or disable NetBIOS over TCP/IP.

The changes take effect immediately without rebooting the system.

Optionally, if you are using a DHCP server that can selectively enable and disable NetBIOS configurations through DHCP option types, you can choose the Use NetBIOS setting from the DHCP server. NetBIOS over TCP/IP can also be disabled for computers that are running Windows 2000/2003 by using the advanced DHCP option types that are supported by the Windows 2000/2003 DHCP Server service.

Note Computers that are running an operating system prior to Windows 2000 will be unable to browse, locate, or create file and print share connections to a Windows 2000/XP/2003 computer with NetBIOS disabled.

Configuring ACS 4.2 Enhanced Logging Features

ACS 4.2 provides several new logging features. When you configure the CSV Failed Attempts and Passed Authentications reports, you can add several new fields:

- **Response Time**—Indicates how long it takes ACS to respond to a client after receiving an authentication request.
- **Framed-IP-address**—If ACS is configured to assign IP addresses when it receives Access-Request messages or if an incoming Access-Request contains an IP address, indicates the framed IP address.
- **Session-ID**—Indicates the session ID of a user session.

To add a field to the CSV Failed Attempts or Passed Authentications report:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **Logging**.

The Logging Configuration page opens.

Step 3 In the CSV column, click **Configure** next to the name of the report you want to configure.

The configuration page for the selected report opens.

Step 4 To add a field to the report, click the field name in the Attributes column and then click the right arrow button to move it to the Logged Attributes column.

Step 5 Click **Submit** to save the report configuration.

Configuring Group Filtering at the NAP Level

You can use ACS 4.2 to grant and deny access to users who are authenticated through a LDAP database based on the LDAP group to which the users belong. This feature is called group filtering at the NAP level.

To configure group filtering at the NAP level:

Step 1 Configure LDAP on the ACS server.

Step 2 Set up a Network Access Profile.

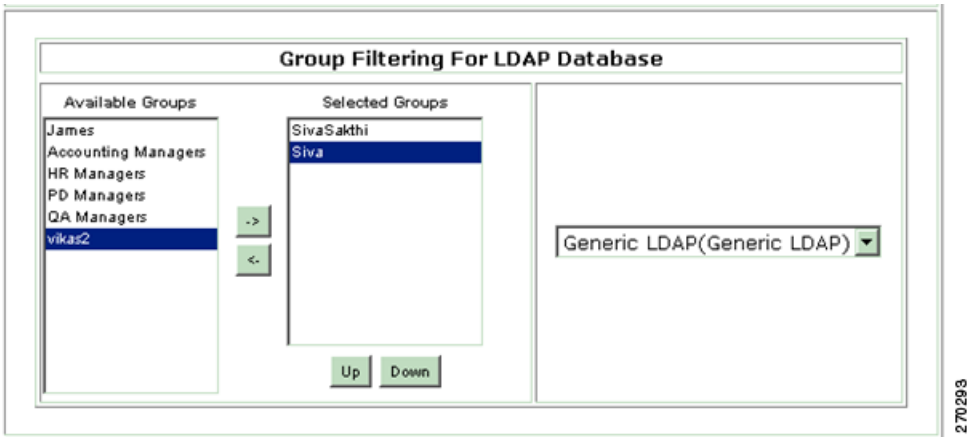
a. In the navigation bar, click **Network Access Profiles**.

The Network Access Profile page opens.

b. Click the **Authentication** link for the profile.

The Authentication page for the selected profile appears. The top of the Authentication page contains the Group Filtering for LDAP database section, as shown in Figure 3-3.

Figure 3-3 Group Filtering for LDAP Database Configuration



c. From the drop-down list for LDAP databases, choose the LDAP database that you want to use to filter user access.

d. From the list of LDAP user groups in the Available Groups list, choose the groups for which to allow access.

Choose a group in the Available Groups list and click the right arrow (-->) button to move the group to the list of Selected Groups.

e. If you want to sort the lists, click the **Up** and **Down** buttons to move a group up or down in a list.

Step 3 Click **Submit**.

Option to Not Log or Store Dynamic Users

When ACS authenticates users by using external databases, such as Active Directory or LDAP, and a user is successfully authenticated with the external database, then, by default, ACS stores the information for the user in the ACS internal database. The users that ACS creates in this manner are called dynamic users.

With ACS 4.2, you can configure ACS not to not create or store data on dynamic users.

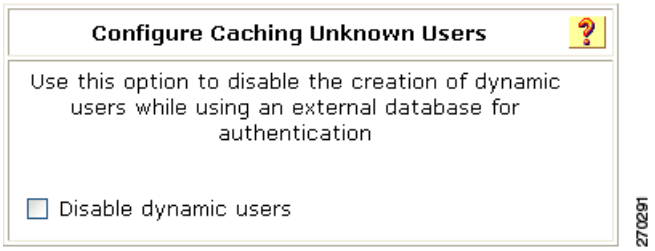
To disable creation of dynamic users in the ACS internal database:

Step 1 In the navigation bar, choose **External User Databases > Unknown User Policy**.

The Configure Unknown User Policy page opens.

Step 2 Scroll down to the Configure Caching Unknown Users section, shown in Figure 3-4:

Figure 3-4 Disabling Creation of Dynamic Users



Step 3 Check the **Disable Dynamic users** check box.

Step 4 Click **Submit**.

Active Directory Multi-Forest Support

ACS supports machine authentication in a multi-forest environment. Machine authentications succeed as long as an appropriate trust relation exists between the primary ACS forest and the requested domain's forest. When a requested user's or machine's domain is part of a trusted forest, machine authentication will succeed.

ACS supports user authentication between multiple forests for EAP-FAST, version1a with PEAP, MSPEAP, and for EAP-TLS.

Note The multi-forest feature works only where the username contains the domain information.

Configuring Syslog Time Format in ACS 4.2

ACS SE 4.2 provides a new option for configuring the time format that ACS uses to send messages to syslog servers.

In previous releases, ACS SE devices could only send syslog messages using the local time that is set on the ACS device. With release 4.2, you can configure the ACS SE to send syslog messages by using the local time setting or Greenwich Mean Time (GMT).

To configure the time format used for events sent to a syslog server:

Step 1 In the navigation bar, choose **System Configuration > Date Format Control**.

The Date Format Control page opens.

Step 2 In the Time Zone Selection for syslog section, specify the date format for events sent to syslog servers. To specify:

- Local time, click the **Use Local Time** radio button.
- GMT time, click the **Use GMT Time** radio button.

Step 3 Click **Submit and Restart**.

RSA Support on the ACS SE

ACS 4.2 adds support for RSA Token Server on the ACS SE. To add this support:

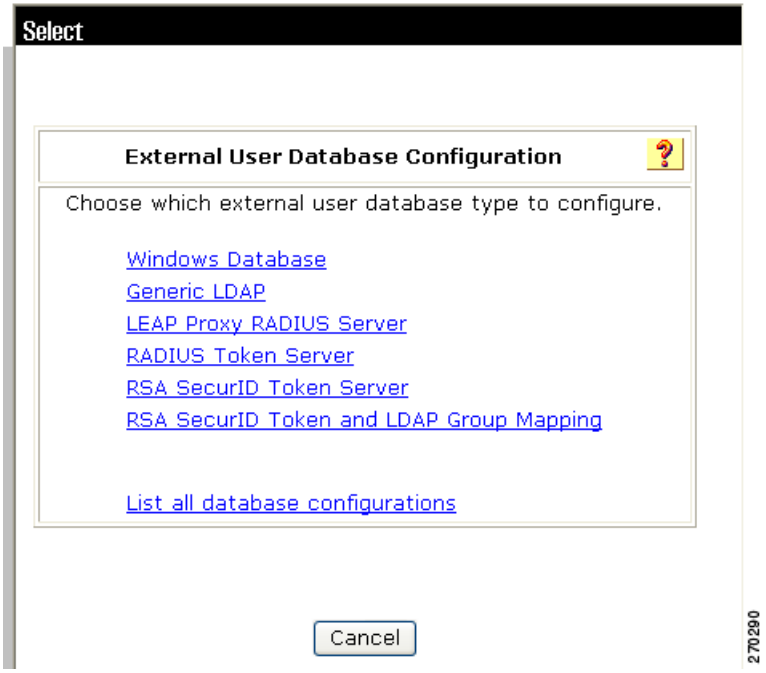
Step 1 In the navigation bar, click **External User Databases**.

The External User Databases page opens.

Step 2 Click **Database Configuration**.

The External User Databases Configuration page opens, as shown in Figure 3-5.

Figure 3-5 External User Databases Page (ACS SE)



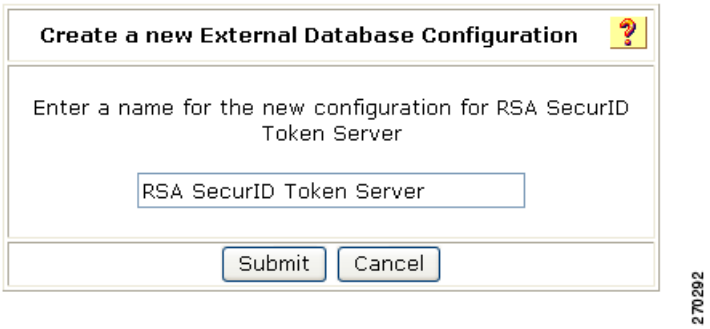
Step 3 Click **RSA SecureID Token Server**.

The Database Configuration Creation page appears.

Step 4 Click **Create New Configuration**.

The Create a New External Database Configuration page appears, as shown in Figure 3-6.

Figure 3-6 Create a New External Database Configuration Page.



Step 5 Enter the name for the RSA SecureID Token Server and then click **Submit**.

You are prompted to choose what to do with the Token Sever.

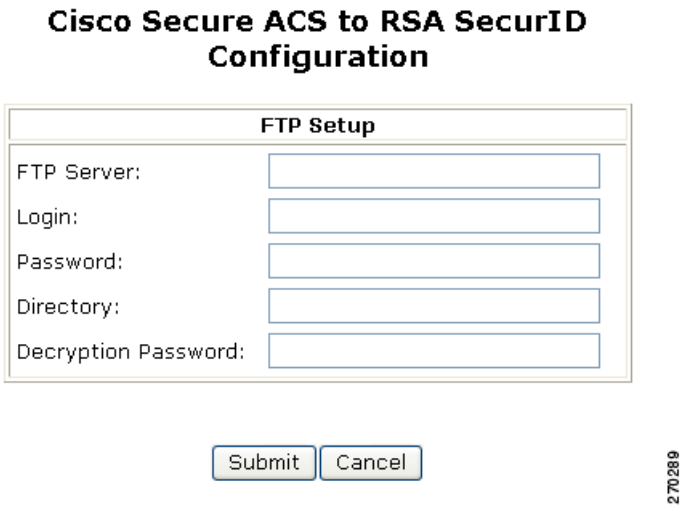
Step 6 Click **Configure**.

You are prompted to upload the *sdconf.rec* file.

Step 7 Click **Upload scconf.rec.**

Step 8 The Cisco Secure ACS to RSA SecurID Configuration page appears, as shown in Figure 3-7.

Figure 3-7 Cisco Secure ACS to RSA SecurID Configuration Page



Step 9 On the Cisco Secure ACS to RSA SecurID Configuration page, enter the information shown in Table 3-3

Table 3-3 RSA SecureID Server Configuration

Field	Description
FTP Server:	The IP address of the FTP server that contains the *sdconf.rec* file. This the configuration file for your RSA TokenID installation.
Login:	The login name for the FTP server.
Password:	The password for the FTP server.
Directory:	The directory on the FTP server where the *sdconf.rec* file is located.

Step 10 Click **Submit**.

Purging the RSA Node Secret File

When you change the RSA Token Server configuration, you must purge the existing Node Secret file. To purge the Node Secret file:

Step 1 In the navigation bar, click **External User Databases**.

The External User Databases page opens.

Step 2 Click **Database Configuration**.

The External User Databases Configuration page opens.

Step 3 Click **RSA SecurID Token Server**.

The External User Database Configuration page opens.

Step 4 Click **Configure**.

The Cisco Secure ACS to RSA SecurID Configuration page opens.

Step 5 Click **Purge Node Secret**.

Configuring RSA SecurID Token and LDAP Group Mapping

You can perform authentication with RSA in native mode and also by using LDAP group mapping, with RSA. If you use RSA with LDAP group mapping, then the user's LDAP group membership controls authorization. When RSA native mode authentication succeeds, group mapping occurs with LDAP. The user's group is applied based on the group mapping configuration.

Note Before you configure RSA authentication with LDAP Group Mapping, ensure that you have the correct installation or configuration of the third-party DLLs required to support this type of external database.

To configure RSA authentication with LDAP Group Mapping:

Step 1 Enable RSA support as described in RSA Support on the ACS SE, page 3-8.

Step 2 In the navigation bar, click **External User Databases**.

Step 3 Click **Database Configuration**.

ACS lists all possible external user database types.

Step 4 Click **RSA SecurID Token and LDAP Group Mapping**.

The External Database Configuration page appears.

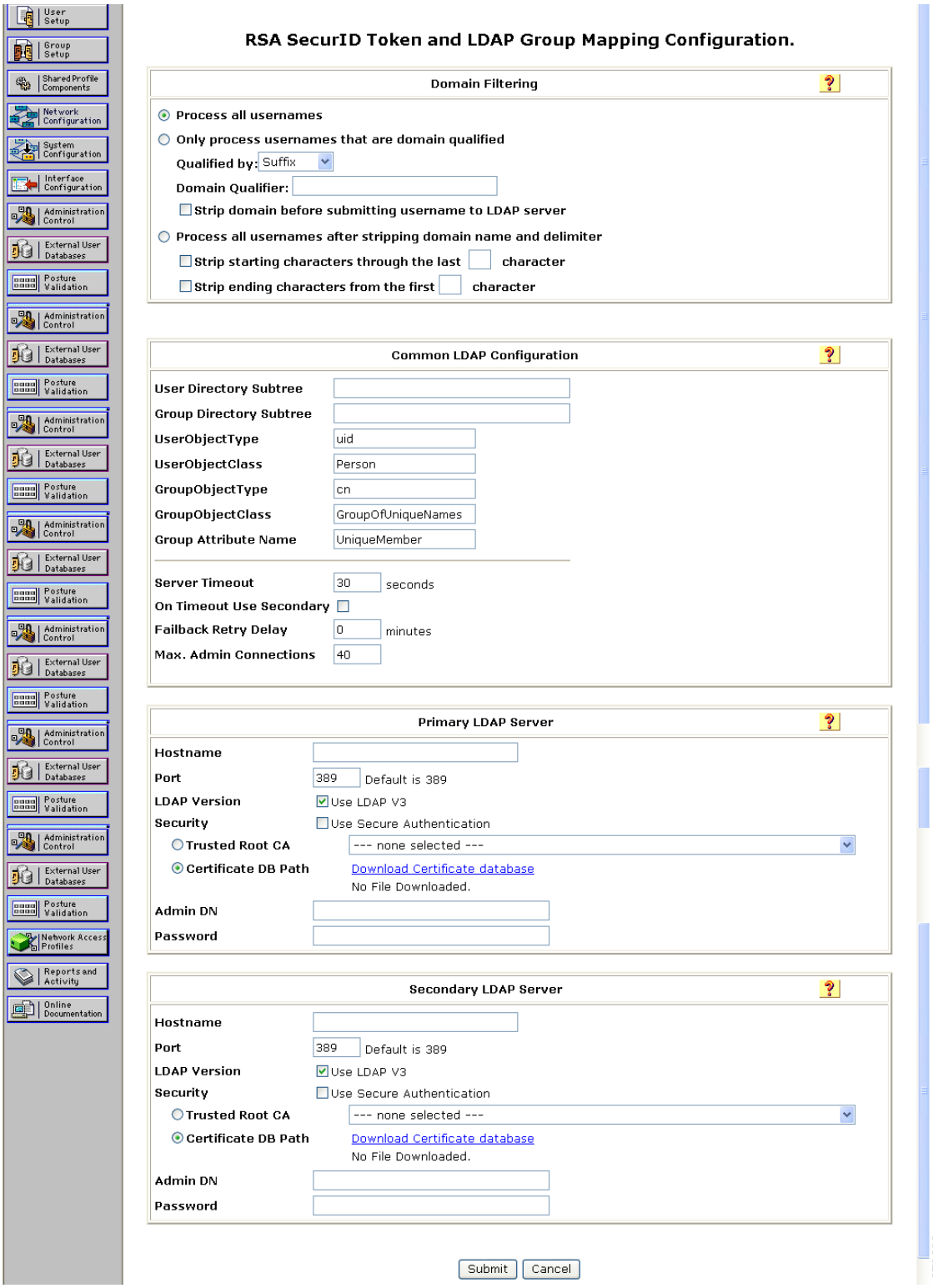
Step 5 Click **Configure.**

The LDAP Native RSA Configuration page opens.

Step 6 Click **Configure LDAP**.

The RSA SecurID Token and LDAP Group Mapping Configuration page opens, as shown in Figure 3-8.

Figure 3-8 RSA SecurID Token and LDAP Group Mapping Configuration Page



Step 7 If you do not want ACS to filter LDAP authentication requests by username, under Domain Filtering, choose **Process all usernames**.

Step 8 If you want to limit authentications processed by this LDAP configuration to usernames with a specific domain qualification:

Note For information about domain filtering, see "Domain Filtering" in chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*.

a. Under Domain Filtering, click the **Only process usernames that are domain qualified** radio button.

b. From the Qualified by list, choose the applicable type of domain qualification: Suffix or Prefix. Only one type of domain qualification is supported per LDAP configuration.

   For example, if you want this LDAP configuration to authenticate usernames that begin with a specific domain name, select **Prefix**. If you want this LDAP configuration to authenticate usernames that end with a specific domain name, select **Suffix**.

c. In the Domain Qualifier box, type the name of the domain for which you this LDAP configuration should authenticate usernames. Include the delimiting character that separates the user ID from the domain name. Ensure that the delimiting character appears in the applicable position: at the end of the domain name if **Prefix** is selected on the Qualified by list; at the beginning of the domain name if Suffix is selected on the Qualified by list.

   Only one domain name is supported per LDAP configuration. You can type up to 512 characters.

d. If you want ACS to remove the domain qualifier before submitting it to the LDAP database, check the **Strip domain before submitting username to LDAP server** check box.

e. If you want ACS to pass the username to the LDAP database *without* removing the domain qualifier, uncheck the **Strip domain before submitting username to LDAP server** check box.

Step 9 If you want to enable ACS to strip domain qualifiers from usernames before submitting them to an LDAP server:

Note For information about domain filtering, see "Domain Filtering" in chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*.

a. Under Domain Filtering, click the **Process all usernames after stripping domain name and delimiter** radio button.

b. If you want ACS to strip prefixed domain qualifiers, check the **Strip starting characters through the last *X* character** check box, and then type the domain-qualifier delimiting character in the *X* box.

Note The *X* box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the *X* box contains any of these characters, stripping fails.

c. If you want ACS to strip suffixed domain qualifiers, check the **Strip ending characters from the first *X* character** check box, and then type the domain-qualifier delimiting character in the *X* box.

Note The *X* box cannot contain the following special characters: the pound sign (#), the question mark (?), the quote (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). ACS does not allow these characters in usernames. If the *X* box contains any of these characters, stripping fails.

Step 10 Under Common LDAP Configuration, in the User Directory Subtree box, type the DN of the tree containing all your users.

Step 11 In the Group Directory Subtree box, type the DN of the subtree containing all your groups.

Step 12 In the User Object Type box, type the name of the attribute in the user record that contains the username. You can obtain this attribute name from your Directory Server. For more information, refer to your LDAP database documentation.

Note The default values in the UserObjectType and following fields reflect the default configuration of the Netscape Directory Server. Confirm all values for these fields with your LDAP server configuration and documentation.

Step 13 In the User Object Class box, type the value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, while others are shared with other object types. Choose a value that is not shared.

Step 14 In the GroupObjectType box, type the name of the attribute in the group record that contains the group name.

Step 15 In the GroupObjectClass box, type a value for the LDAP `objectType` attribute in the group record that identifies the record as a group.

Step 16 In the GroupAttributeName box, type the name of the attribute of the group record that contains the list of user records who are a member of that group.

Step 17 In the Server Timeout box, type the number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server has failed.

Step 18 To enable failover of LDAP authentication attempts, check the **On Timeout Use Secondary** check box.

Step 19 In the Failback Retry Delay box, type the number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first.

Note To specify that ACS should always use the primary LDAP server first, type zero (0) in the Failback Retry Delay box.

Step 20 In the Max. Admin Connection box, enter the number of maximum concurrent connections with LDAP administrator account permissions.

Step 21 For the Primary LDAP Server and Secondary LDAP Server tables:

Note If you did not check the **On Timeout Use Secondary** check box, you do not need to complete the options in the Secondary LDAP Server table.

a. In the Hostname box, type the name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.

b. In the Port box, type the TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port 636 is usually used.

c. To specify that ACS should use LDAP version 3 to communicate with your LDAP database, check the **LDAP Version** check box. If the LDAP Version check box is not checked, ACS uses LDAP version 2.

d. If you want ACS to use SSL to connect to the LDAP server, check the **Use secure authentication** check box and complete the next three steps. If you do not use SSL, the username and password credentials are normally passed over the network to the LDAP directory in clear text.

e. ACS SE only: If you checked the **Use Secure Authentication** check box, perform one of the following procedures:. Check the:

- **Trusted Root CA** check box, and in the adjacent drop-down list, choose a **Trusted Root CA**.
- **Certificate Database Path** check box, and download a *cert7.db* file.

Note To download a *cert7.db* certificate database file to ACS now, complete the steps in "Downloading a Certificate Database (Solution Engine Only)" in Chapter 12 of the *User Guide for Cisco Secure ACS, 4.2*, and then continue with Step f. You can download a certificate database later. Until a certificate database is downloaded for the current LDAP server, secure authentication to this LDAP server fails.

f. ACS for Windows only: If you checked the **Use Secure authentication** check box, perform one of the following procedures. Click the:

- **Trusted Root CA** radio button, and in the adjacent drop-down list, choose a **Trusted Root CA**.
- **Certificate Database Path** radio button, and in the adjacent box, type the path to the Netscape *cert7.db* file, which contains the certificates for the server to be queried and the trusted CA.

g. The Admin DN box requires the fully qualified Distinguished Name (DN) of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory subtree.

In the Admin DN box, type the following information from your LDAP server:

uid=*user id*`,[ou=`*organizational unit*`,]`
`[ou=`*next organizational unit*`]o=`*organization*

where *user id* is the username

organizational unit is the last level of the tree

next organizational unit is the next level up the tree.

For example:

```
uid=joesmith,ou=members,ou=administrators,o=cisco
```

Tip If you are using Netscape DS as your LDAP software, you can copy this information from the Netscape console.

h. In the Password box, type the password for the administrator account that is specified in the Admin DN box. The server determines password case sensitivity.

Step 22 Click **Submit**.

Note ACS saves the generic LDAP configuration that you created. You can now add it to your Unknown User Policy or assign specific user accounts to use this database for authentication.

Turning Ping On and Off

With ACS 4.2, you can enable and disable pinging of the ACS SE device. Prior to release 4.2, when remote devices sent a ping request to an SE device, the ping was always rejected because, by default, the Cisco Security Agent (CSA) runs on the ACS SE device. CSA automatically rejects remote ping requests.

ACS 4.2 provides software patches for you to turn ping on and off by updating the policies in the CSA:

- **Ping Turn On Patch**—This patch turns on the ping option in the CSA, which makes it possible to ping the ACS SE.
- **Ping Turn Off Patch**—This patch turns off the ping option in the CSA, which causes the ACS SE to reject pings.

For detailed information on installing these patches, see "Turning Ping On and Off" in Chapter 3 of the the *Installation Guide for Cisco Secure ACS Solution Engine, 4.2*, "Installing and Configuring Cisco Secure ACS Solution Engine 4.2."

CHAPTER 4

Using RDBMS Synchronization to Create dACLs and Specify Network Configuration

This chapter describes how to configure ACS 4.2 to enable new RDBMS Synchronization features introduced with ACS 4.2.

For detailed information on RDBMS Synchronization, see "RDBMS Synchronization" in Chapter 8 of the *User Guide for Cisco Secure ACS, 4.2*, "System Configuration: Advanced."

For detailed information on the accountActions codes to use with RDBMS Synchronization, see Appendix E of the *User Guide for Cisco Secure ACS, 4.2*, "RDBMS Synchronization Import Definitions."

This chapter contains:

New RDBMS Synchronization Features in ACS Release 4.2

ACS 4.2 provides enhanced support for RDBMS Synchronization:

- **Configuration of Downloadable ACLs (dACLs) for Specified Users and Groups**—You can specify dACLs by entering **permit ip** and **deny ip** commands in a comma-separated value (CSV) *accountActions* file. By using new account action codes that you include in the *accountActions* file, you can create a dACL that contains the commands that the text file specifies.

  On ACS for Windows, you can perform dACL configuration from the RDBMS Synchronization page in the ACS GUI or by running the **CSDBSync** command.

  On the ACS SE, you can perform dACL configuration from the RDBMS Synchronization page in the ACS SE GUI; or, connect to the ACS SE by using an SSH client and then running the **csdbsync -syncnow** command from the SSH shell.

- **Support for Creation, Reading, Updating, and Deleting of Single or Multiple AAA Clients Through RDBMS Synchronization**—With the capability to read AAA client data, you can export the AAA client list for a particular NDG, an AAA client list with a specified IP range, or the list of all AAA clients.

- **Remote Invocation of the CSDBSync Service on the ACS Solution Engine**—With ACS 4.2, you can run the **CSDBSync** service on a remote ACS SE, over an SSH connection.

Using RDBMS Synchronization to Configure dACLs

With ACS 4.2, you can use RDBMS Synchronization to set up downloadable dACLs and associate dACLs with specified Users or Groups.

To configure dACLs by using RDBMS Synchronization:

Step 1 Enable RDBMS Synchronization and dACLs.

Step 2 Create a text file to define the dACLs.

Step 3 Code an *accountActions* CSV file to create the dACL, and associate a User or Group with the dACL.

Step 4 Configure RDBMS Synchronization to use a local CSV file.

Step 5 Perform RDBMS Synchronization in one of two ways:

- From the ACS GUI.
- By running the **csdbsync -syncnow** command from the Windows command shell or in an SSH connection with a remote ACS SE.

Step 6 View the dACL.

Step 1: Enable dACLs

To enable dACLs:

Step 1 In the **Navigation Bar**, click **Interface Configuration**.

Step 2 Click **Advanced Options**.

The Advanced Options page opens.

Step 3 Check the **User-Level Downloadable ACLs** check box.

Step 4 Check the **Group-Level Downloadable ACLs** check box.

This enables assigning a dACL to a Group Name.

Step 5 Check the **RDBMS Synchronization** check box.

Step 6 Click **Submit**.

Step 2: Create a Text File to Define the dACLs

To create a text file to define dACLs:

Step 1 Use a text editor of your choice to create a text file; for example Notepad.

Example 4-1 shows a sample text file.

Example 4-1 Sample Text File for Creating a dACL

```
[DACL#1]
Name = DACL_For_Troy
Description = Test_DACL_For_ACS_42
Content#1= content1
Definition#1#1= permit ip any host 192.168.1.152
Definition#1#2= permit ip any host 192.168.5.152
Definition#1#3= permit ip any host 192.168.29.33
Definition#1#4= permit ip any host 192.168.29.34
Definition#1#5= permit ip any host 192.168.9.50
Definition#1#6= permit ip any host 192.168.9.20
Definition#1#7= permit ip any host 192.168.7.20
Definition#1#8= permit ip any host 192.168.128.1
Definition#1#9= permit ip any 192.168.24.0 0.0.0.255
Definition#1#10= permit ip any 192.168.0 0.0.0.255
Definition#1#11= permit ip any 192.0.0.0 0.255.255.255
Definition#1#12= deny ip any 192.168.0.0 0.3.255.255
Definition#1#13= deny ip any 192.168.0.0 0.1.255.255
Definition#1#14= permit ip any any
```

Step 2 Code the information in the file as described in Table 4-1.

Table 4-1 Keywords for Creating a dACL By Coding a Text File

Keyword	Value
dACL number	The first line of the text file must specify the dACL number, enclosed in square brackets; for example, `[DACL#n]`, where *n* is the number of the dACL. In Example 4-1, the first line specifies `DACL#1`, because the file specifies only one dACL.
Name	Specifies the name of the dACL that is created when you run **CSDBSync**.
Description	Specifies a short description of the dACL.
Content	Specifies the number of a content block that consists of definitions for access privileges associated with the dACL. This keyword has the format `Content#n`, where *n* specifies the number of the content block. The file shown in Example 4-1 has only one content block.
Definition keywords	Specify a series of **permit IP** or **deny ip** commands that ACS applies to Users or Groups to which you associate the dACL. Each Definition keyword has the format `Definition #n#n1`, where *n* is the number of the content block of definition keywords and *n1* is the number of each definition.

Step 3 Save the file:

- **ACS for Windows**—Save the file to a directory on the Windows machine that is running ACS.
- **ACS SE**—Save the file to a directory on an FTP server used with the ACS SE.

Step 3: Code an accountActions File to Create the dACL and Associate a User or Group with the dACL

To create a an *AccountActions* CSV file to create a dACL and assign it to a User or Group:

Step 1 Create a text file by using a text editor of your choice; for example, Notepad.

Step 2 Code a statement to create a User or Group. For example, to create a User named *Troy*, who belongs to a Group named *Group*, and has an initial password of *ipassword*, code the following statement:

```
1,1,Troy,Group 5,100,ipassword,7/8/2008 15:00,0,,,0
```

Step 3 Code a statement to create a dACL. For example, to create a dACL called *DACL_for_Troy* that is specified in a text file called *dACL_create.txt*, code the following statement:

```
2,1,,,385,C:\dACL_folder\dACL_create.txt,7/8/2008 15:00,0,,,0
```

Action code 385 creates a dACL. The value directly after the action code specifies the directory path and filename of the text file that specifies the dACL. In the sample code shown in Example 4-1 and Example 4-2, this is the *dACL_create.txt* file.

The value after the directory path and filename must specify a timestamp for the file; for example, `7/8/2008 15:00.`

Step 4 Code a statement to associate the dACL with a specified User. For example, to associate the dACL *DACL_for_Troy* with the User *Troy*, code:

```
3,1,Troy,,380,DACL_For_Troy,7/8/2008 15:00,0,,,0
```

The third value in this statement specifies the User (*Troy*) to associate the dACL with. Action code 380 associates dACL with the User, and the value immediately after the action code specifies the dACL name (*dACL_for_Troy*).

The value after the dACL name must specify a timestamp for the action; for example, `7/8/2008 15:00.`

Step 5 Save the file:

- **ACS for Windows**—Save the file to a directory on the Windows machine that is running ACS.
- **ACS SE**—Save the file to a directory on an FTP server used with the ACS SE.

Sample *accountActions* CSV File

Example 4-2 shows a sample *accountActions* CSV file.

Note The default filename for the CSV is *accountactions.csv*. However, you can rename it.

Example 4-2 Sample accountActions CSV File

```
SequenceId,Priority,UserName,GroupName,Action,ValueName,DateTime,MessageNo,ComputerNames,A
ppId,Status
1,1,Troy,Group 5,100,ipassword,7/8/2008 15:00,0,,,0
2,1,,,385,C:\dACL_folder\dACL_create.txt,7/8/2008 15:00,0,,,0
3,1,Troy,,380,DACL_For_Troy,7/8/2008 15:00,0,,,0
```

Table 4-2 describes the accountActions codes used in Example 4-2 to add a User, create a dACL, and associate the dACL with a specified User or Group.

Table 4-2 Account Action Codes to Create dACLs and Assign Them to Specified Users or Groups

Action Code	Name	Required	Description
100	ADD_USER	UN|GN, V1	Creates a User (32 characters maximum). The variable *V1* is used as the initial password. Optionally, you can assign the User to a Group.
385	CREATE_DACL	VN	Use this action code to create a dACL. VN = <*input_file_name*> where *input_file_name* is a text file that contains definitions for dACLs. On ACS for Windows, this file resides in a directory on the Windows machine that is running ACS. On the ACS SE, this file resides on an FTP server used with the ACS SE. You can specify the absolute file path; for example: *C:\DACL\create_DACL_for_User_1.txt* for ACS for Windows. The dACL definition is ignored if it is already present, or contains an invalid definition, content name, content definition, or NAF name.
380	CREATE_USER_DACL	UN|GN, VN	This action code associates a specified dACL with a User or Group. The dACL name specified should be valid and present in ACS. The codes are: UN = valid Username GN = Valid Group name (optional) VN = dACL name. (This dACL must be defined in Shared Profile Components).

Step 4: Configure RDBMS Synchronization to Use a Local CSV File

To configure RDBMS Synchronization to use a local CSV file:

Step 1 In the navigation bar, click **System Configuration**.

Step 2 Click **RDBMS Synchronization**.

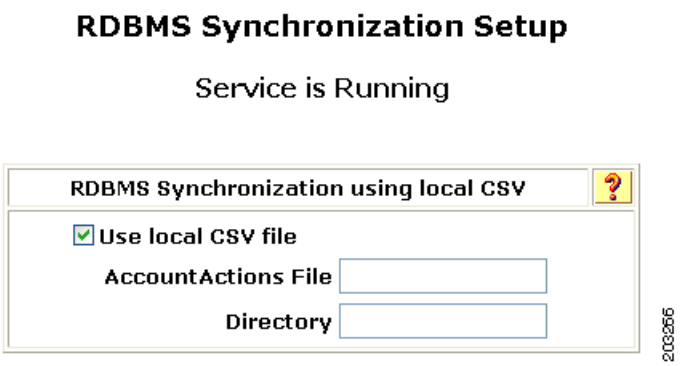
Note If this feature does not appear, choose **Interface Configuration > Advanced Options**, then check the **RDBMS Synchronization** check box.

The RDBMS Synchronization Setup page appears.

Step 3 If you are using ACS for Windows, complete these steps:

a. Complete the required fields on the RDBMS Synchronization Setup page (Figure 4-1).

Figure 4-1 RDBMS Synchronization Setup Page (ACS for Windows)



b. Check the **Use local CSV file** check box.

c. In the AccountActions file field, enter the filename of the *accountActions* CSV file that you created in Step 3: Code an accountActions File to Create the dACL and Associate a User or Group with the dACL, page 4-4.

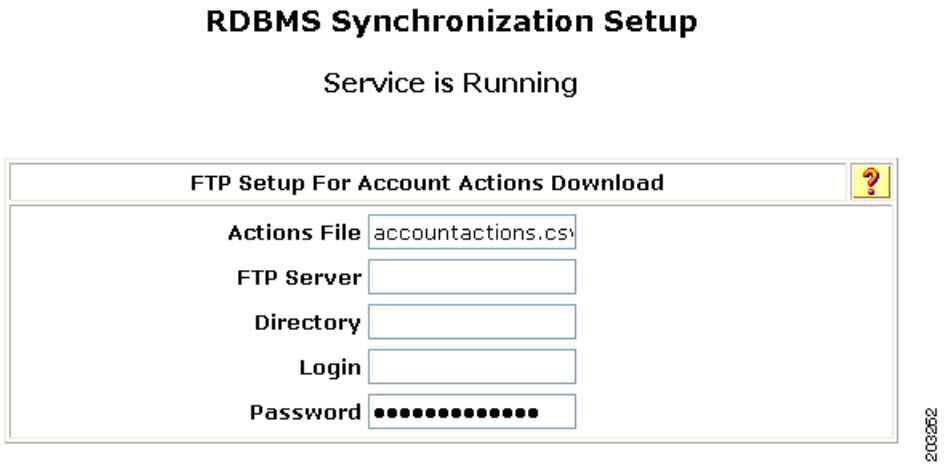
d. In the Directory field, enter the directory path to the *accountActions* CSV file.

ACS has the information with which to access the accountActions table.

Step 4 If you are using ACS SE:

a. Complete the required fields on the RDBMS Synchronization Setup page (Figure 4-2).

Figure 4-2 RDBMS Synchronization Setup Page (ACS SE)



b. Enter the following information:

- **Actions File**— The name of the *accountActions* file. The default name is *accountactions.csv*. The filename provided must match the name of the *accountActions* file on the FTP server.
- **FTP Server**—The IP address or hostname of the FTP server from which ACS obtains the *accountActions* file. If you specify a hostname, DNS must be enabled on your network.
- **Directory**—The relative path from the FTP server root directory to the directory where the *accountActions* file resides. To specify the FTP root directory, enter a single dot (.).
- **Username**—A valid username to enable ACS to access the FTP server.

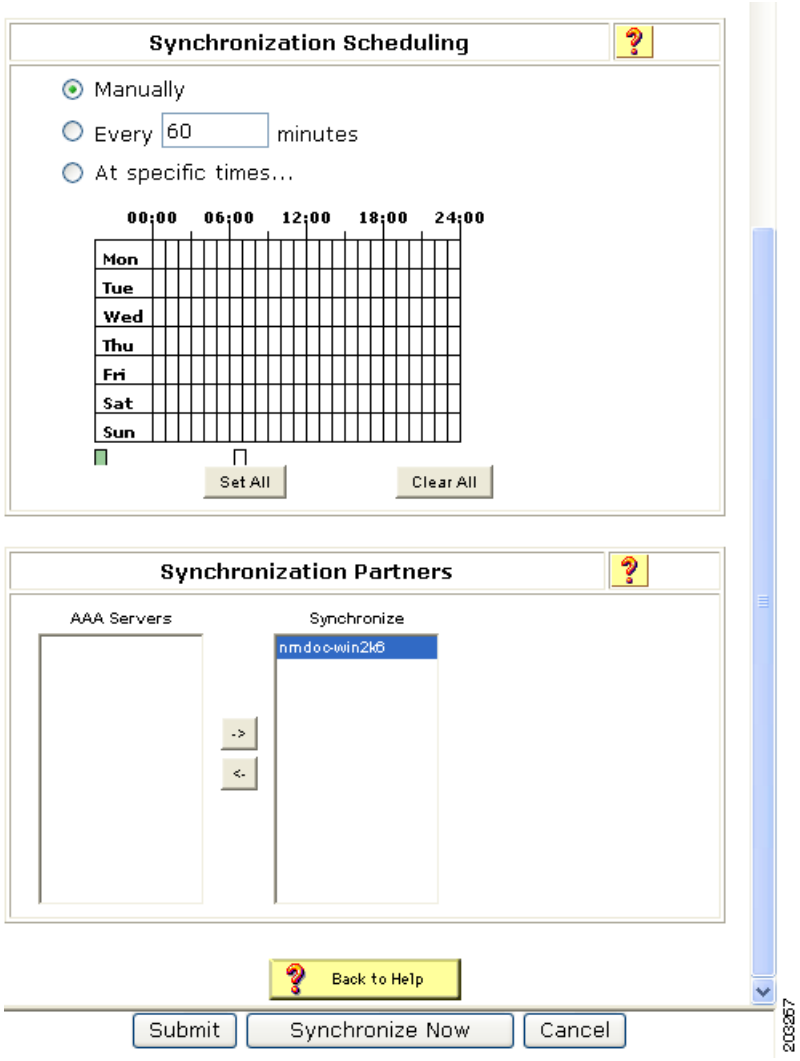
- **Password**—The password for the username provided in the Login box.

The ACS SE has the information necessary to get the *accountActions* file from the FTP server.

Step 5 (ACS for Windows and ACS SE) Set the Synchronization Scheduling and Synchronization Partners options as required.

Figure 4-3 shows the Synchronization Scheduling and Synchronization Partners sections of the RDBMS Synchronization Setup page.

Figure 4-3 Synchronization Scheduling and Synchronization Partners Options



Step 6 Specify the following Synchronization Scheduling information:

- **Manually**—If you want to disable automatic RDBMS Synchronization, check the **Manually** check box.
- **Every** *X* **minutes**—ACS performs synchronization on a set frequency. The unit of measurement is minutes, with a default update frequency of 60 minutes.
- **At specific times**—ACS performs synchronization at the time that is specified in the day and hour graph. The minimum interval is one hour, and the synchronization occurs on the hour that you chose.

Step 7 For each ACS that you want this ACS to update with data from the accountActions table, click the ACS in the AAA Servers list, and then click the right arrow button (-->) on the interface.

The ACS that you chose appears in the Synchronize list.

Step 8 To remove ACSs from the Synchronize list, click the ACS in the Synchronize list, and then click the left arrow button (**<--**).

The ACS that you chose is removed from the Synchronize list.

Step 9 At the bottom of the browser window, click **Synchronize Now**.

ACS immediately begins a synchronization event. To check the status of the synchronization, view the RDBMS Synchronization report in Reports and Activity.

Step 5: Perform RDBMS Synchronization

You can perform the RDBMS Synchronization and create the dACLs in two ways. By running:

- RDBMS Synchronization from the ACS GUI.
- **CSDBSync** manually to create the dACLs.

Running RDBMS Synchronization from the ACS GUI

When you click **Synchronize Now** on the RDBMS Synchronization page for ACS for Windows or for the ACS SE, ACS begins a synchronization event and creates the dACLs specified in the *accountActions* CSV file.

Running CSDBSync Manually to Create the dACLs

You can run **CSDBSync** manually to create the dACLs.

ACS for Windows

In Windows, use the command line interface to invoke the **csdbsync -run** command.

The **CSDBSync** service reads each statement from the *accountActions* CSV file and updates the ACS internal database as the action codes in the file specify. In a distributed environment, a single ACS, known as the senior synchronization partner, accesses the accountActions table and sends synchronization commands to its synchronization partners.

Step 1 Open a command prompt window.

Step 2 Enter the following commands:

a. To stop the **CSDBSync** service, enter `net stop csdbsync`.

b. Enter `net start csdbsync.`

c. Enter one of the following commands:

- `csdbsync -run`
- `csdbsync -syncnow`

ACS fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Synchronization operations that the file specifies.

ACS SE

On the ACS SE, you can run the **csdbsync -syncnow** command to invoke RDBMS Synchronization

To run **CSDBSync** manually on the ACS SE:

Step 1 Check connectivity between the ACS SE and the FTP server, and be certain that you have write permissions to the FTP server directory.

Step 2 Start a SSH command shell.

Step 3 Enter the following commands:

a. To stop the **CSDBSync** service, enter `net stop csdbsync`.

b. Enter `net start csdbsync.`

c. Enter one of the following commands:

- `csdbsync -run`
- `csdbsync -syncnow`

ACS SE fetches the CSV file from the database, reads the action codes in the file, and performs the RDBMS Synchronization operations that file specifies.

Performing RDBM Synchronization Using a Script

On the ACS SE, you can change ACS configuration from a remote system by using a command-line utility for RDBMS Synchronization that includes SSH support. You can use the mechanism that starts the SSH server to add Administrator privileges and invoke the **csdbsync -syncnow** command. The **csdbsync -syncnow** and **csdbsync -run** commands work the same, without stopping or starting the **CSDBSync** service.

You can include the commands to perform these actions in a script that you run remotely on a specified ACS SE.

Step 6: View the dACLs

After you have run RDBMS Synchronization to create the dACLs, view the dACLs to ensure that they are correct.

To view the dACLs:

Step 1 In the **Navigation Bar**, click **Shared Profile Components**.

Step 2 Click **Downloadable IP ACLs**.

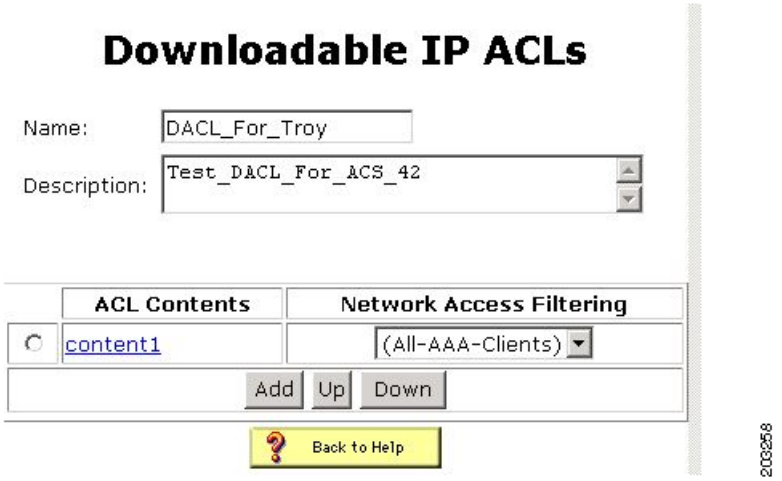
The Downloadable IP ACLs page opens

In the Name column of the Downloadable IP ACLs table, you should see the dACL that was specified in the text file that you coded in Step 2: Create a Text File to Define the dACLs, page 4-2.

Step 3 Click the name of the dACL.

The Downloadable IP ACLs page displays the selected dACL, as shown in Figure 4-4.

Figure 4-4 Entry for the Sample dACL

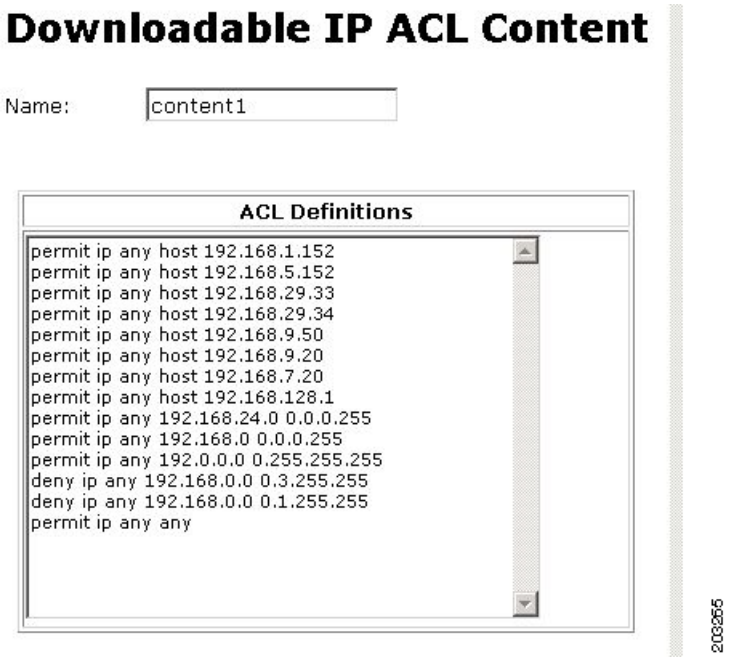


In the ACL Contents column, you should see the content name specified in the Content#1 block that you coded in the text file in Step 2: Create a Text File to Define the dACLs, page 4-2.

Step 4 Click the content name.

The Downloadable IP ACL Content page appears. The Content Name and ACL Definitions appear on the page, as shown in Figure 4-5.

Figure 4-5 Downloadable IP ACL Content Page



Step 5 If the dACL was not created correctly, review the steps in Using RDBMS Synchronization to Configure dACLs, page 4-2 and check for errors.

For a list of error messages, see Error Messages, page 4-11.

Error Messages

Table 4-3 lists the error messages associated with dACL creation using **CSDBSync**.

Table 4-3 dACL Creation Errors

Error Message	Explanation
Failed to process DACL. DACL not defined.	**Possible Cause** The dACL was not specified correctly in the text file used to define the dACLs. **Recommended Action** Review the text file that you coded to specify the dACLs and ensure that the syntax is correct.
Failed to process DACL. Could not find NAF.	**Possible Cause** The text file provided to define the dACL did not correctly define a NAF. **Recommended Action** Review the text file that you coded to specify the dACLs and ensure that the syntax is correct.
Failed to process DACL. Failed to get UserID.	**Possible Cause** On the ACS SE, the user ID specified for the FTP server in the RDBMS Synchronization configuration was incorrect. **Recommended Action** Check to ensure that the specified user ID exists on the FTP server used with the ACS SE.
Failed to process DACL. DACL content not found.	**Possible Cause** The text file used to specify the dACL did not correctly specify the dACL content. **Recommended Action** Check the syntax in the text file and ensure that it is correct. Ensure that the ACLs defined in the file are correct.
Failed to upload file into FTP server.	**Possible Cause** The FTP server was not reachable, or a network error occurred. **Recommended Action** Ensure that the IP address for the FTP server in the RDBMS configuration is correct and that the network is functioning correctly.

Table 4-3 dACL Creation Errors (continued)

Error Message	Explanation
Failed to import DACL file.	**Possible Cause** The user ID specified in the RDBMS Synchronization configuration does not have write access to the ACS. **Recommended Action** Ensure that the specified user has write access to the ACS.
Failed to access Host DB.	**Possible Cause** The **CSDBSync** service could not access the database on the host ACS. **Recommended Action** Ensure that the database on the ACS is configured correctly and enabled correctly in the ACS GUI.

Reading, Updating, and Deleting dACLs

Table 4-4 lists the account action codes that you can use to read, update, or delete a dACL.

Table 4-4 Account Action Codes for Creating, Reading, Updating, or Deleting dACLs

Action Code	Name	Required	Description
386	READ_DACL	VN, V1 (optional)	Use this action code to read dACL attributes and save them in a file for later use. VN = contains dACL name or * for all dACLs. V1 = <*output_file_name*> where *output_file_name* contains the exported dACLs definition. On the ACS SE, *output_file_name* specifies the file in the FTP server for the ACS SE. If not is specified the default filename *DumpDACL.txt* is used. On ACS for Windows, you can specify the absolute file path; for example, *C:\temp\DACL.txt* for ACS for Windows. If you do not specify the file path and filename, ACS writes the data to a file in the *ACS\bin* directory.
387	UPDATE_DACL	VN, V1(optional)	Use this action code to update dACL attributes. VN = <*input_file_name*> where *input_file_name* specifies the file that contains the definition for the dACL to be updated. On the ACS SE platform, *input_file_name* specifies the file name present in the FTP server for ACS SE. You can specify the absolute file path; for example: *C:\DACL\dump.txt* for ACS for Windows. V1=DACL_REPLACE or DACL_APPEND The default option is: DACL_REPLACE The DACL_REPLACE option replaces the existing dACL with the new one. DACL_APPEND appends the new dACL content and its definition to the existing dACL. If the dACL has not been defined, the new dACL is added to the existing list. The dACL definition is ignored if it contains an invalid definition, content name, content definition or NAF name.
388	DELETE_DACL	VN	Use this action code to delete a dACL. VN = The name of the dACL to delete. To delete all dACLs, code an asterisk (*). By default, all the dACLs are deleted. Users and Groups associated with this dACL will be dereferenced after deleting the dACL.

Updating or Deleting dACL Associations with Users or Groups

Table 4-5 lists the account action codes to update the dACL or remove the association of the dACL and the User or Group.

Table 4-5 Account Action Codes to Create or Remove dACL Associations With Users and User Groups

Action Code	Name	Required	Description
381	UPDATE_USER_DACL	UN|GN, VN	This action code updates the dACL for a specified User or Group. The dACL name specified should be valid and should be present in ACS. UN = Valid Username GN = Valid Group name (optional) VN = dACL name. (This dACL must be defined in Shared Profile Component)
382	DELETE_USER_DACL	UN|GN	This action code disassociates a dACL from a specified User or Group. UN = valid Username GN = Valid Group name (optional)

Using RDBMS Synchronization to Specify Network Configuration

You can use RDBMS Synchronization to perform network configuration tasks, such as:

- Add AAA clients.
- Delete AAA clients.
- Set AAA client configuration details.
- Add AAA servers.
- Delete AAA servers.
- Set AAA server configuration details.
- Add and configure Proxy Distribution Table entries.

Note For specific information about all actions that RDBMS Synchronization can perform, see Appendix E, "RDBMS Synchronization Import Definition," in the *User Guide for Cisco Secure ACS, 4.2*.

Creating, Reading, Updating and Deleting AAA clients

The RDBMS Synchronization feature supports creation and deletion of single or multiple AAA clients. In addition, accountActions codes 224 and 225 enable reading and updating AAA client information. This section describes the various RDBMS Synchronization tasks that you can perform on single or multiple AAA clients.

Table 4-6 lists the account action codes that are used to read and update single or multiple AAA clients.

Table 4-6 Account Action Codes for Create, Read, Update, Delete for AAA Clients

Action Code	Name	Required	Description
224	UPDATE_NAS	VN, V1, V2, V3	Use this action code to update AAA clients. VN = AAA Client Name V1 = IP-Address V2 = Shared Secret Key V3 = Vendor
225	READ_NAS	VN, V1 (optional)	Use this action code to export an AAA client list to an output file that can be used to associate the list with members of a particular NDG or with all AAA clients. You can use this output file as input for **CSUtil**, to import NASs. VN = <*output_file_name*> where *output_file_name* specifies the filename for the FTP server used with the ACS SE. If nothing is specified, the default name *DumpNAS.txt* is used. For the ACS for Windows platform, you can specify the absolute file path; for example: *C:\MyNAS\dump.txt*. If no value is specified, the AAA client lists is written to the *\ACS\bin\DumpNAS.txt* file. V1 = NDG name (optional) V1 should contain a valid NDG name.

CHAPTER 5

Password Policy Configuration Scenario

Cisco Secure ACS, hereafter referred to as ACS, provides new password features to support corporate requirements mandated by the Sarbanes-Oxley Act of 2002. Sarbanes-Oxley (SOX) requires stricter enforcement of password restrictions.

ACS provides SOX support, which includes:

- Enforcement of password lifetime policy
- Enforcement of inactivity limits
- Improved password constraints

To enable password configuration that includes these new features, ACS provides a new password policy page.

All administrator logins are subject to the policy that you configure for passwords and accounts, unless you check the Account Never Expires check box. For example, ACS provides configurable limits on password lifetime and activity, and incorrect password attempts. These options can force password change and can result in automatic account lockout. Privileged administrators can also lock out an account. In addition, you can monitor the last password change and last account activity for each administrator.

Limitation on Ability of the Administrator to Change Passwords

If an administrator is not granted full administrative access, the only action the administrator can take is to change his or her own password.

Summary of Configuration Steps

To configure password policy in ACS:

Step 1 Add a new administrator account.

Add a new administrator account, specify the administrator name and password, and grant access privileges. See Step 1: Add and Edit a New Administrator Account, page 5-2 for details.

Step 2 Configure password policy.

Configure restrictions on the admin user password. See Step 2: Configure Password Policy, page 5-4 for details.

Step 3 Configure session policy.

Configure restrictions on the admin user's session. See Step 3: Configure Session Policy, page 5-7 for details.

Step 4 Configure access policy.

Configure restrictions on admin access, such as the IP addresses from which administrators can log in. See Step 4: Configure Access Policy, page 5-9 for details.

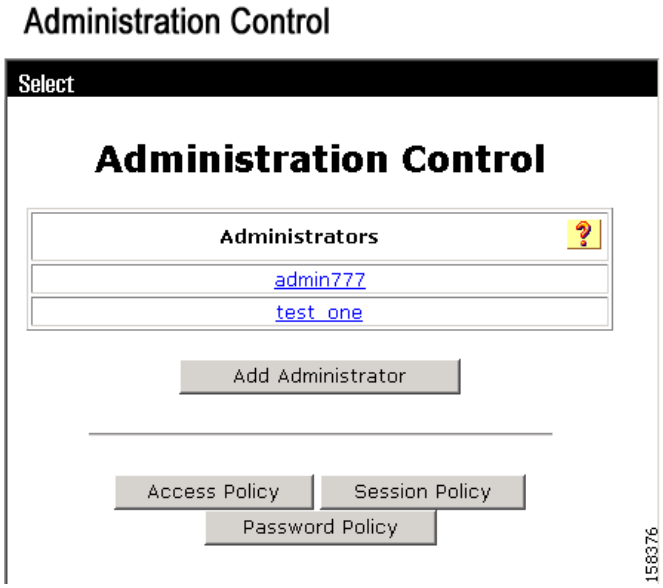
Step 1: Add and Edit a New Administrator Account

To add a new administrator account:

Step 1 In the navigation bar, click **Administration Control.**

The Administration Control page appears, as shown in Figure 5-1.

Figure 5-1 Administration Control Page



The Administration Control page initially lists no administrators. If administrators have been configured, the page lists the configured administrators.

Step 2 To add an administrator, click **Add Administrator.**

The Add Administrator page opens.

Step 3 In the Administrator Details area, enter:

Option	Description
Administrator Name	Enter the login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, excluding the left angle bracket (<), the right angle bracket (>), and the backslash (\). An ACS administrator name does not have to match a network user name.
Password	Enter the password for the administrator to access the ACS web interface. The password can match the password that the administrator uses for dial-in authentication; or, it can be a different password. ACS enforces the options in the Password Validation Options section on the Administrator Password Policy page. Passwords must be at least 4 characters long and contain at least 1 numeric character. The password cannot include the username or the reverse username, must not match any of the previous 4 passwords. and must be in ASCII characters. For errors in passwords, ACS displays the password criteria. If the password policy changes and the password does not change, the administrator remains logged in. ACS enforces the new password policy at the next login.
Confirm Password	Reenter the password that you entered in the password field.

Option	Description
Account Never Expires	If you want to override the lockout options set up on the Administrator Password Policy page (with the exception of manual lockout), check the check box next to Account Never Expires. If you check this option, the account never expires but password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	If you want to lock out an administrator who is denied access due to the account policy options specified on the Password Policy page, check the check box for **Account Locked**. When unchecked (disabled), this option unlocks an administrator who was locked out. Administrators who have the Administration Control privilege can use this option to manually lock out an account or reset locked accounts. The system displays a message that explains the reason for a lockout. When an administrator unlocks an account, ACS resets the Last Password Change and the Last Activity fields to the day on which the administrator unlocks the account. The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.

Step 4 Click **Grant All** or **Revoke All** to globally add or remove all privileges,

Step 5 If you want to grant specific privileges to the administrator, check the check boxes that correspond to the privileges that you want to grant.

Note For more information on administrative privileges, see the "Add Administrator and Edit Administrator Pages" section in Chapter 11 of the *User Guide for Cisco Secure Access Control Server 4.2*, "Administrators and Administrative Policy."

Step 6 Go to Step 2: Configure Password Policy, page 5-4 (the next section of this chapter) and follow the steps to specify password restrictions.

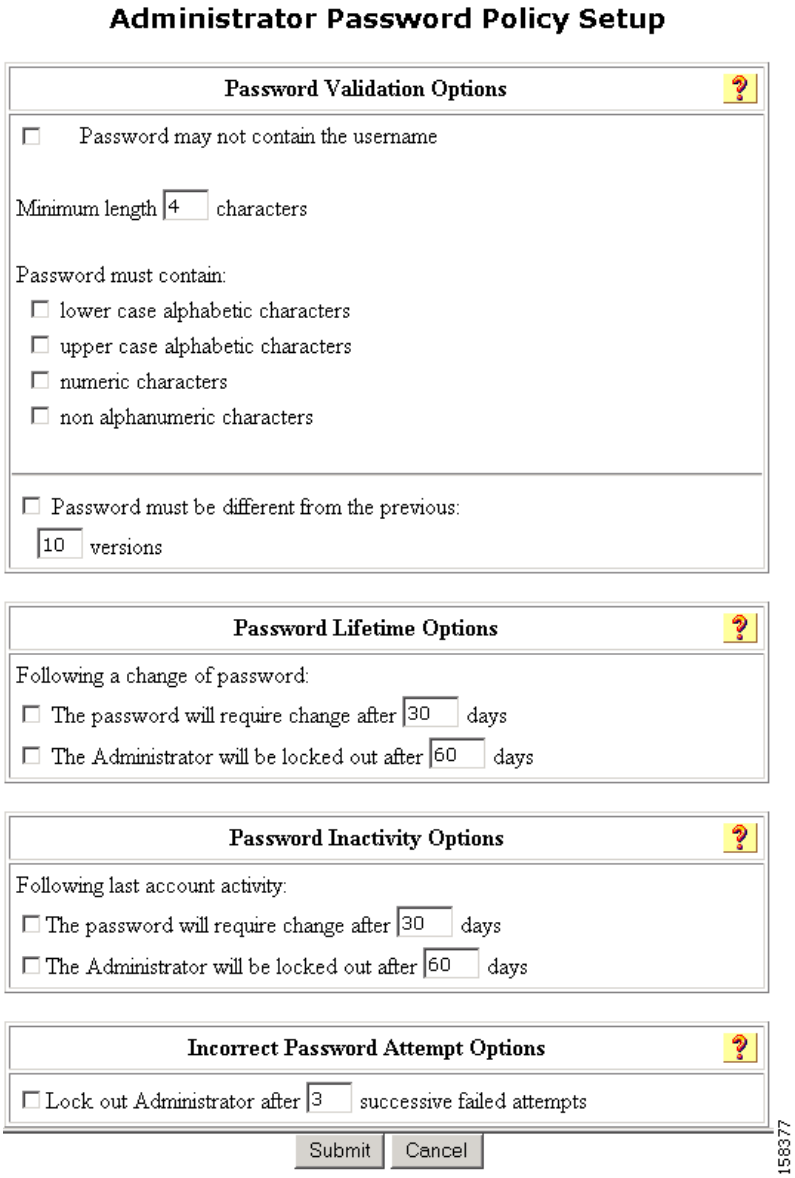
Step 2: Configure Password Policy

To configure password policy:

Step 1 On the Administration Control page, click **Password Policy**.

The Administrator Password Policy Setup page appears, shown in Figure 5-2.

Figure 5-2 The Administrator Password Policy Setup Page



Step 2 On the Password Policy Setup Page, specify:

- Password Validation Options

  See Specify Password Validation Options, page 5-6.
- Password Lifetime Options

  See Specify Password Lifetime Options, page 5-6.
- Password Inactivity Options

  See Specify Password Inactivity Options, page 5-7.
- Incorrect Password Attempt Option

  See Specify Incorrect Password Attempt Options, page 5-7.

Specify Password Validation Options

In the Password Validation Options section, configure:

- **Password may not contain the username**—If enabled, the password cannot contain the username or the reverse username.
- **Minimum length *n* characters**—*n* specifies the minimum length of the password (default = 4, range = 4 to 20).
- **Uppercase alphabetic characters**—If enabled, the password must contain uppercase alphabetic characters.
- **Lowercase alphabetic characters**—If enabled, the password must contain lowercase alphabetic characters.
- **Numeric characters**—If enabled, the password must contain numeric characters.
- **Non alphanumeric characters**—If enabled, the password must contain nonalphanumeric characters; for example, the at symbol (@).
- **Password must be different from the previous *n* versions**—If enabled, the password must be different from the previous *n* versions (default = 10, range = 0 to 99).

Specify Password Lifetime Options

In the Password Lifetime Options section, configure:

- **The password will require change after *n* days**—Following a change of password, if this option is enabled, *n* specifies the number of days before ACS requires a change of password due to password age (the default value is 30 days). The range is 1 to 365. When checked (enabled), the Administrator will be locked after *n* days option causes ACS to compare the two password lifetime Options and use the greater value of the two.
- **The Administrator will be locked out after *n* days**—Following a change of password, if this option is enabled, *n* specifies the number of days before ACS locks out the associated administrator account due to password age. The default value is 30 days; the range is1 to 365 days.

Specify Password Inactivity Options

In the Password Inactivity Options section, configure:

- **The password will require change after *n* days**—Following the last account activity, if enabled, *n* specifies the number of days before ACS requires a change of password due to password inactivity The default value is 30 days; the range is 1 to 365 days. When checked (enabled), the Administrator will be locked after *n* days option causes ACS to compare the two Password Inactivity Options and use the greater value of the two.

Note For additional security, ACS does not warn users who are approaching the limit for password inactivity.

- **The Administrator will be locked out after *n* days**—Following the last account activity, if enabled, *n* specifies the number of days before ACS locks out the associated administrator account due to password inactivity (default = 30, range = 1 to 365).

Note For additional security, ACS does not warn users who are approaching the limit for account inactivity.

Specify Incorrect Password Attempt Options

In the Incorrect Password Attempt Options section, configure:

Lock out Administrator after *n* successive failed attempts—If checked (enabled), *n* specifies the allowable number of incorrect password attempts. When checked, *n* cannot be set to zero (0). If not checked (disabled), ACS allows unlimited successive failed login attempts. The default value is 3 days; the range = 1 to 98 days.

Note For additional security, ACS does not warn users who are approaching the limit for failed attempts. If the **Account Never Expires** option is checked (enabled) for a specific administrator, this option is ignored.

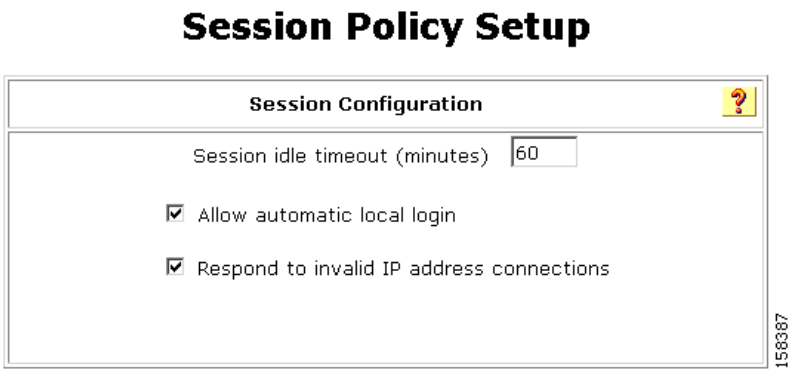
Step 3: Configure Session Policy

To configure session policy:

Step 1 On the Administration Control page, click **Session Policy**.

The Session Policy Setup page opens, as shown in Figure 5-3.

Figure 5-3 The Session Policy Setup Page



Step 2 On the Session Policy Setup page, set session options as required.

You can specify:

- **Session idle timeout (minutes)**—Specifies the time, in minutes, that an administrative session must remain idle before ACS terminates the connection (4-character maximum).

  When an administrative session terminates, ACS displays a dialog box asking whether the administrator wants to continue. If the administrator chooses to continue, ACS starts a new administrative session.

  This parameter only applies to the ACS administrative session in the browser. It does not apply to an administrative dial-up session.

- **Allow Automatic Local Login (ACS for Windows Only**—Enables administrators to start an administrative session without logging in, if they are using a browser on the computer that runs ACS. ACS uses a default administrator account named *local_login* to conduct these sessions.

  When unchecked (disabled), administrators must log in by using administrator names and passwords.

Note To prevent accidental lockout when there are no defined administrator accounts, ACS does not require an administrator name and password for local access to ACS.

  The local_login administrator account requires the Administration Control privilege. ACS records administrative sessions that use the local_login account in the Administrative Audit report under the local_login administrator name.

- **Respond to invalid IP address connections**—Enables ACS to send an error message in response to attempts to start a remote administrative session by using an IP address that is invalid according to the IP address range settings in the Access Policy. If this check box is unchecked, ACS does not display an error message when a user makes an invalid remote connection attempt. This option is checked (enabled) by default.

  Disabling this option can help to prevent unauthorized users from discovering ACS.

Step 4: Configure Access Policy

This section describes how to configure administrative access policy.

Before You Begin

If you want to enable the SSL for administrator access, you must have completed the steps in Install the CA Certificate, page 7-4, and Add a Trusted Certificate, page 7-4. After you have enabled SSL, ACS begins using the SSL at the next administrator login. This change does not affect current administrator sessions. In the absence of a certificate, ACS displays an error message when you attempt to configure SSL.

To set up an ACS access policy:

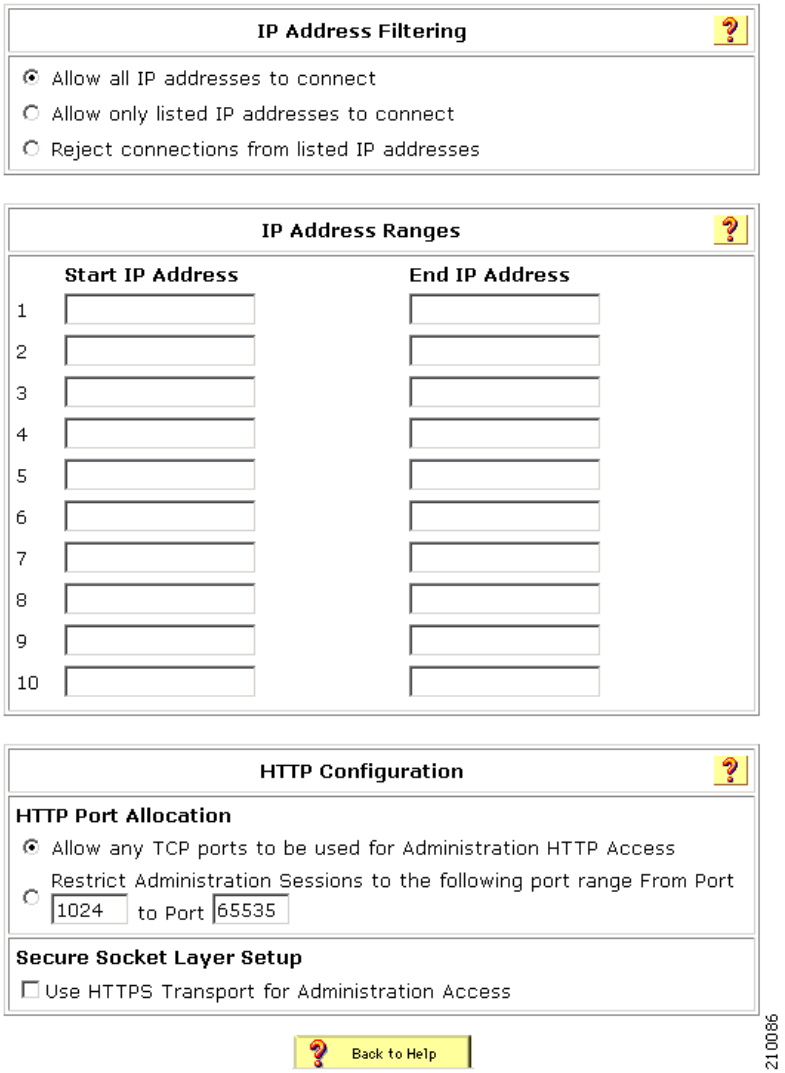
Step 1 In the navigation bar, click **Administration Control**.

ACS displays the Administration Control page.

Step 2 Click **Access Policy**.

The Access Policy Setup page appears, as shown in Figure 5-4.

Figure 5-4 Access Policy Setup Page



Step 3 Click the appropriate **IP Address Filtering** option

Table 5-1 Access Policy Options

Option	Description
IP Address Filtering	
Allow all IP addresses to connect	Enables remote access to the web interface from any IP address.
Allow only listed IP addresses to connect	Restricts remote access to the web interface to IP addresses within the specified IP Address Ranges.

Table 5-1 Access Policy Options (continued)

Option	Description
Reject connections from listed IP addresses	Restricts remote access to the web interface to IP addresses outside of the specified IP Address Ranges. IP filtering operates on the IP address received in an HTTP request from a remote administrator's web browser. If the browser is configured to use an HTTP proxy server or the browser runs on a workstation behind a network device performing network address translation, IP filtering applies only to the IP address of the HTTP proxy server or the NAT device.
IP Address Ranges	The IP Address Ranges table contains ten rows for configuring IP address ranges. The ranges are always inclusive; that is, the range includes the Start and End IP addresses. Use dotted-decimal format. The IP addresses that define a range must differ only in the last octet (Class C format).
Start IP Address	Defines the lowest included IP address in the specified range (up to 16 characters).
End IP Address	Defines the highest included IP address in the specified range (up to 16 characters).
HTTP Configuration	
HTTP Port Allocation	
Allow any TCP ports to be used for Administration HTTP Access	Enables ACS to use any valid TCP port for remote access to the web interface.
Restrict Administration Sessions to the following port range From Port *n* to Port *n*	Restricts the ports that ACS can use for remote access to the web interface. Use the boxes to specify the port range (up to five digits per box). The range is always inclusive; that is, the range includes the start and end port numbers. The size of the specified range determines the maximum number of concurrent administrative sessions. ACS uses port 2002 to start all administrative sessions. Port 2002 does not need to be in the port range. Also, ACS does not allow definition of an HTTP port range that consists only of port 2002. The port range must consist of at least one port other than port 2002. A firewall configured to permit HTTP traffic over the ACS administrative port range must also permit HTTP traffic through port 2002, because this is the port that a web browser must address to initiate an administrative session. We do not recommend allowing administration of ACS from outside a firewall. If access to the web interface from outside a firewall is necessary, keep the HTTP port range as narrow as possible. A narrow range can help to prevent accidental discovery of an active administrative port by unauthorized users. An unauthorized user would have to impersonate, or "spoof," the IP address of a legitimate host to make use of the active administrative session HTTP port.

Table 5-1 Access Policy Options (continued)

Option	Description
Secure Socket Layer Setup	
Use HTTPS Transport for Administration Access	Enables ACS to use the secure socket layer (SSL) protocol to encrypt HTTP traffic between the **CSAdmin** service and the web browser that accesses the web interface. This option enables encryption of all HTTP traffic between the browser and ACS, as reflected by the URLs, that begin with HTTPS. Most browsers include an indicator for SSL-encrypted connections. To enable SSL, first install an a server certificate and a certification authority certificate. Choose **System Configuration > ACS Certificate Setup** to access the installation process. With SSL enabled, ACS begins using HTTPS at the next administrator login. Current administrator sessions are unaffected. In the absence of a certificate, ACS displays an error.

Step 4 Type the appropriate IP address ranges in accordance with the IP Address Filtering option.

Step 5 Click the appropriate HTTP Port Allocation option to allow all ports or restrict access to certain ports. If you restrict access, type the range of the restricted ports.

Step 6 Check this option if you want ACS to use the SSL.

Step 7 Click **Submit**.

ACS saves and begins enforcing the access policy settings.

Viewing Administrator Entitlement Reports

To assist in SOX compliance, ACS produces entitlement report, which contain data extracted from the ACS configuration and formatted into text based files.

ACS produces entitlement reports for administrators and users. The reports that you can generate are:

- **Privilege**—The privileges granted to a selected administrator.
- **Combined Privilege**—The privileges granted to all administrators.
- **Users to Groups Mapping**—The group membership of every user.

View Privilege Reports

To view privilege reports:

Step 1 In the navigation bar, click **Reports and Activity**.

The Reports page opens.

Step 2 Click **Entitlement Reports**.

A list of the available entitlement reports appears. Figure 5-5 shows an example list.

Figure 5-5 List of Entitlement Reports

Step 3 To view a report, click the report name.

Each report is downloaded to the local computer in the form of an Excel spreadsheet.

CHAPTER 6

Agentless Host Support Configuration Scenario

This chapter describes how to configure the agentless host feature in Cisco Secure Access Control Server, hereafter referred to as ACS.

Note The procedure in this chapter describes how to configure agentless host support by using ACS with a Lightweight Directory Access Protocol (LDAP) database. You can also configure agentless host support by using the ACS internal database: but, using an LDAP database is generally more efficient.

This chapter contains the following sections:

Overview of Agentless Host Support

Many hosts that ACS authenticates run agent software that requests access to network resources and receives authorization from ACS. However, some hosts do not run agent software. For example:

- Many 802.1x port security deployments authenticate hosts that do not have appropriate security agent software, such as Cisco Trust Agent.
- When an agentless host is connected to a Layer 2 device and an Extensible Authentication Protocol over User Datagram Protocol timeout (EoU timeout) occurs, in-band posture validation cannot occur.

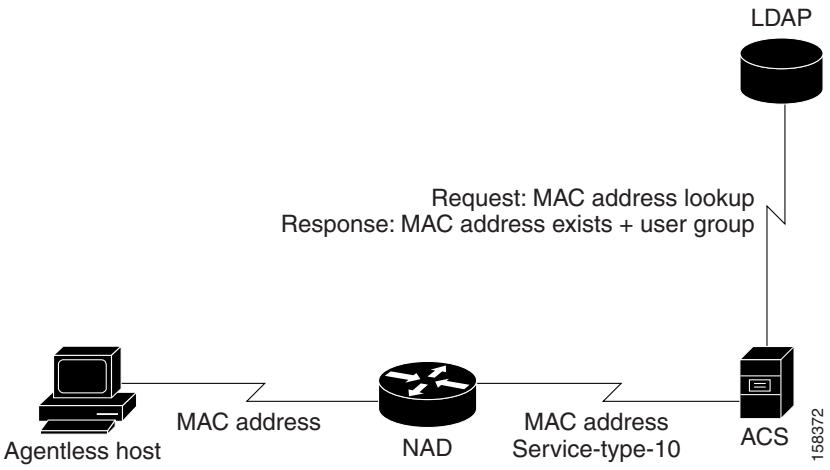
ACS solves this problem by using the MAC address of the host device to identify and authenticate the host. This technique is called MAC authentication bypass (MAB).

1. When an agentless host connects to a network access device (NAD), the NAD detects that the host does not have an appropriate software agent and uses the host's MAC address to identify it.
2. The NAD sends ACS a RADIUS authorization request with `servicetype=10` and the MAC address of the host contained in the `calling-station-id` attribute.

3. If you configure ACS for MAB, it searches the authentication database for the host's MAC address The database can be:
   - ACS internal
   - LDAP (if you configure LDAP)
4. During the database lookup:
   - ACS looks up the MAC address in an identity store (the internal ACS database or an LDAP database).
   - ACS maps the MAC address to an ACS user group.
   - If ACS finds the MAC address, ACS associates the access request to an ACS user group.
   - If ACS does not find the MAC address, ACS assigns the access request to a default group that has been configured for failed MAB. At this stage, ACS proceeds with authorization as for all other access requests.
   - The expected value in the `calling-station-id attribute` is a MAC address; however, if the attribute contains a different value (IP address), ACS looks for the IP address in the access database
   - ACS applies authorization rules based on the user group and associated policies that a Network Access Profile contains.

Figure 6-1 shows the flow of MAB information.

Figure 6-1 MAB Flow



Using Audit Servers and GAME Group Feedback

You can configure ACS to use audit servers. An audit server is a device that checks the information that the NAD provides against a list of predetermined device types.

The audit server can categorize an end device and provide additional information to ACS. ACS can then make a group assignment decision based on the categorization of the device. For example, if the device is a printer, ACS can assign the device to a user group that includes printers.

In a Cisco Network Admission Control (NAC) environment, ACS supports audit server authentication by enabling Generic Authorization Message Exchange (GAME) group feedback.

GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server.

To use the GAME group feedback feature, you must add a NAC attribute-value pair to the ACS RADIUS dictionary before configuring a posture validation policy that uses GAME group feedback.

You then configure a posture validation policy in a NAP that requests device type authentication from the audit server. For details on configuring posture validation, see Enable Posture Validation, page 7-46.

The detailed steps for configuring GAME group feedback are described in Enable GAME Group Feedback, page 7-46 in Chapter 9, "NAC Configuration Scenario."

Summary of Configuration Steps

To configure agentless host support in ACS:

Step 1 Install ACS for Windows or ACS Solution Engine (ACS SE).

See Step 1: Install ACS, page 6-4 for details.

Step 2 Configure a RADIUS AAA client.

See Step 2: Configure a RADIUS AAA Client, page 6-5 for details.

Configure restrictions on the admin user password.

Step 3 Install and set up an ACS security certificate:

Note This step is required to enable posture validation and Network Access Profiles.

a. Obtain certificates and copy them to the ACS host.
b. Run the Windows certificate import wizard to install the certificate
c. Enable security certificates on the ACS installation.
d. Install the CA certificate.
e. Add a trusted certificate.

See Step 3: Install and Set Up an ACS Security Certificate, page 6-6 for details.

Step 4 Configure LDAP support for MAB:

a. Configure an external LDAP database for MAB support.
b. Create One or More LDAP Database Configurations in ACS.

See Step 4: Configure LDAP Support for MAB, page 6-10 for details.

Step 5 Configure user groups for MAB segments.

See Step 5: Configure User Groups for MAB Segments, page 6-17 for details.

Step 6 Enable agentless request processing:

a. Create a new Network Access Profile.
b. Enable agentless host processing for the profile.
c. Configure MAB.

See Step 6: Enable Agentless Request Processing, page 6-18 for details.

Step 7 Configure logging and reports.

Add the **Bypass Info** attribute to the Passed Authentications and Failed Attempts reports. See Step 7: Configure Logging and Reports, page 6-23.

Note If you are using ACS with NAC, configure audit server support and, optionally, configure GAME group feedback. See Configure GAME Group Feedback, page 6-24 for details.

Basic Configuration Steps for Agentless Host Support

This section describes the basic configuration steps for agentless host support.

Step 1: Install ACS

This section describes the installation process that you perform to run ACS, which runs on a Windows 2000 Server, a Windows 2003 system, or a Cisco Secure ACS SE.

To install ACS:

Step 1 Start ACS installation.

For detailed information on ACS installation, refer to the:

- *Installation Guide for Cisco Secure ACS for Windows 4.2*
- *Installation Guide for Cisco Secure ACS Solution Engine 4.2*

During the installation process, you are prompted to enter a password for encrypting the internal database.

Step 2 Enter a password that is at least 8 characters long, and contains letters and numbers.

The ACS installation process for ACS for Windows automatically creates a shortcut to the ACS administrative GUI on your desktop.

Note If you are installing ACS on the ACS SE, you must manually create an administrative GUI user by using the use the **add-guiadmin** command to create a GUI account. For information on this command, see Appendix A of the *Installation Guide for Cisco Secure ACS Solution Engine 4.2*, "Command Reference." You can then access the administrative GUI through a supported browser. For a list of supported browsers, see *Supported and Interoperable Devices and Software Tables for Cisco Secure ACS Solution Engine Release 4.1.*

Step 3 Double-click the ACS Admin icon to open a browser window to the ACS administrative GUI.

Step 4 If you do not see the ACS Admin icon on the desktop, open your browser from the machine on which you installed ACS and go to one of the following locations:

- http://*IP_address*:2002
- http://*hostname*:2002

where *IP_address* is the IP address of the host that is running ACS and hostname is the *hostname* of the host that is running ACS.

Step 2: Configure a RADIUS AAA Client

Before you can configure agentless host support, you must configure a RADIUS AAA client.

To configure a RADIUS AAA client:

Step 1 In the navigation bar, click **Network Configuration**.

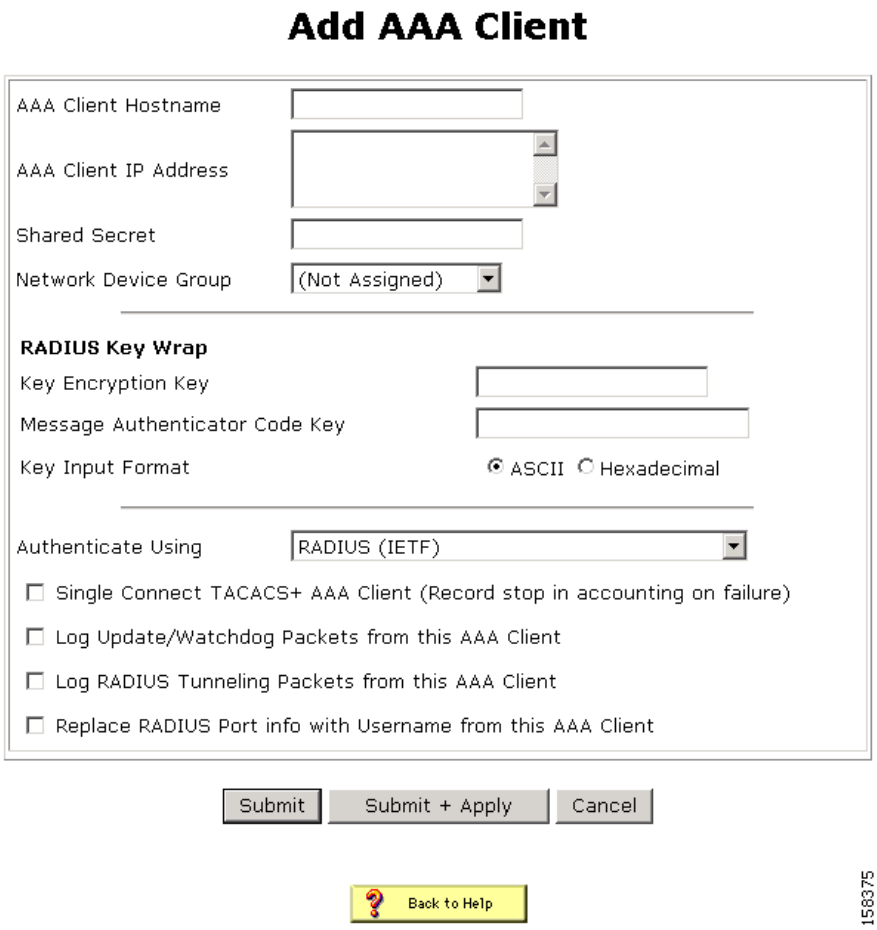
The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using Network Device Groups (NDGs), click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
- To add AAA clients when you have not enabled NDGs, click **Add Entry** below the AAA Clients table.

The Add AAA Client page opens, shown in Figure 6-2.

Figure 6-2 Add AAA Client Page



Step 3 In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 alphanumeric characters).

Step 4 In the AAA Client IP Address box, type the AAA client IP address or addresses.

Step 5 If you are using NDGs, from the Network Device Group list, select the name of the NDG to which this AAA client should belong, or select **Not Assigned** to set this AAA client to be independent of NDGs

Step 6 From the Authenticate Using list, select **RADIUS (IOS/PIX)**.

Step 7 Specify additional AAA client settings as required.

Step 8 Click **Submit + Apply**.

Step 3: Install and Set Up an ACS Security Certificate

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates, and also for information on how to install certificates on the Cisco Secure ACS SE platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, "Advanced Configuration: Authentication and Certificates."

The steps in this section are required to enable posture validation, which is used in Network Access Profiles.

Obtain Certificates and Copy Them to the ACS Host

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\Certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

`mkdir <`*`selected_drive`***`>:\Certs`**

where *`selected_drive`* is the currently selected drive.

Step 3 Copy the following files to the *\Certs* directory:

- *server.cer* (server certificate)
- *server.pvk* (server certificate private key)
- *ca.cer* (CA certificate)

Run the Windows Certificate Import Wizard to Install the Certificate (ACS for Windows)

To run the Windows Certificate Import wizard to install the certificate on the server:

Step 1 Start Windows Explorer.

Step 2 Go to <*selected_drive*>:*Certs*.

where *`selected_drive`* is the currently selected drive.

Step 3 Double-click the *****Certs**ca.cer** file.

The Certificate dialog appears.

Step 4 Select **Install Certificate.**

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.

Step 6 Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, shown in Figure 6-3.

Figure 6-3 Install ACS Certificate Page

Step 5 Ensure that you click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example **`c:\Certs\server.cer.`**

Step 7 In the Private Key File text box, type the server certificate private key location (path and name); for example: **`c:\Certs\server.pvk`**.

Step 8 In the Private Key password text box, type **1111**.

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See Add a Trusted Certificate, page 6-9.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in Figure 6-4.

Figure 6-4 ACS Certification Authority Setup Page

Step 3 In the CA certificate file box, type the CA certificate location (path and name). For example: `c:\Certs\ca.cer`.

Step 4 Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the corresponding check box by the certificate name. For example, find the **Stress** certificate and check the corresponding check box.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click **Restart**.

Step 4: Configure LDAP Support for MAB

You can configure the ACS internal database to manage MAB used with the agentless host feature; however, if you have a large number of MAC addresses to process (for example, several thousand), it is more efficient to use an external LDAP database than to configure the MAC address mappings manually through the ACS GUI.

To configure LDAP support for MAB:

Step 1 Configure an External LDAP database for MAB support.

See Configure an External LDAP Database for MAB Support, page 6-10for details.

Step 2 Create one or more LDAP database configurations in ACS.

See Create One or More LDAP Database Configurations in ACS, page 6-13 for details.

Configure an External LDAP Database for MAB Support

Configure one or more external LDAP databases for MAB support. In each LDAP database, create:

- Device records that describe the agentless hosts that ACS will authenticate.
- LDAP groups that define an LDAP schema to enable MAB for agentless host support.

Example 6-1 shows portions of a sample Lightweight Directory Interchange Format (LDIF) file that defines an LDAP database for agentless host support.

Example 6-1 Sample LDAP Schema for MAB Support

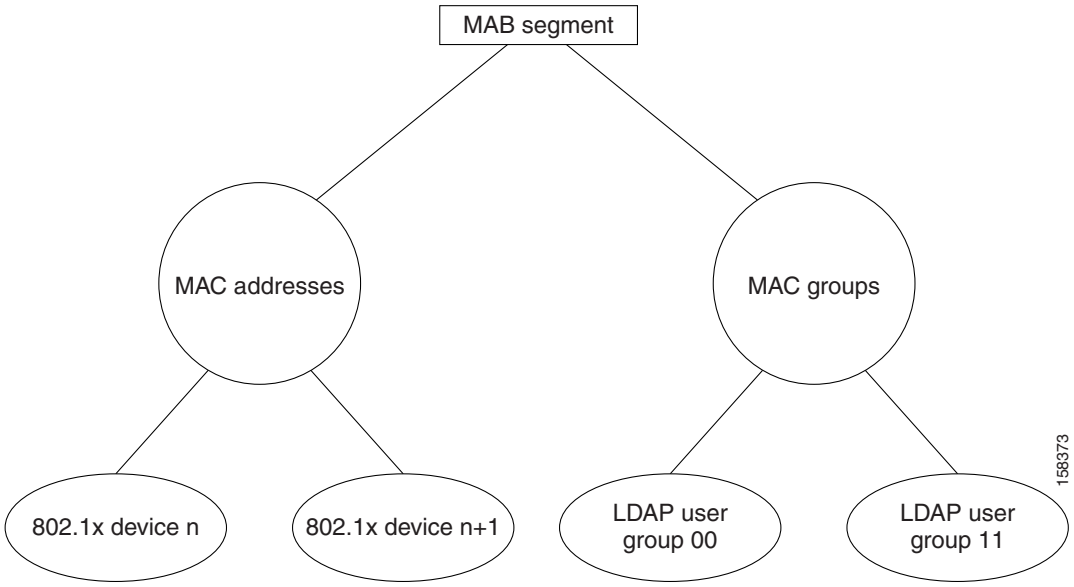
```
dn: ou=MAB Segment, o=mycorp
ou: MAB Segment
objectClass: top
objectClass: organizationalUnit
description: MAC Authentication Bypass Sub-Tree

dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit

dn: cn=user00-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.100
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
macAddress: 00:11:22:33:44:55
cn: user00-wxp.emea.mycorp.com

dn: cn=user11-wxp.emea.mycorp.com,ou=MAC Addresses, ou=MAB Segment, o=mycorp
ipHostNumber: 10.56.60.111
objectClass: top
objectClass: ipHost
objectClass: ieee802Device
```

```
macAddress: 11-22-33-44-55-66
cn: user11-wxp.emea.mycorp.com

dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
cn: Group_1_colon

dn: cn=Group_2_dash,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of - delimited MAC Addresses
uniqueMember: cn=user11-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
uniqueMember: cn=user77b-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
cn: Group_2_dash
```

Description of the Settings in the Sample LDAP Schema

Figure 6-5 shows the tree structure of the LDAP schema that is presented in Example 6-1.

Figure 6-5 Tree Structure for a MAB Support LDAP Schema



How the Subtrees Work

The sample LDAP schema in Example 6-1 contains code to define two subtrees:

```
dn: ou=MAC Addresses, ou=MAB Segment, o=mycorp
ou: MAC Addresses
objectClass: top
objectClass: organizationalUnit

dn: ou=MAC Groups, ou=MAB Segment, o=mycorp
ou: MAC Groups
objectClass: top
objectClass: organizationalUnit
```

The LDAP subtrees are:

- **MAC Addresses**—A user directory subtree that contains device records that specify MAC addresses for agentless hosts (IEEE 802.1x devices that require agentless host authentication by ACS).

  When you specify a user directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the user directory subtree in your LDAP schema in the User Directory Subtree text box.

- **MAC Groups**—A group directory subtree that contains LDAP user groups of users who connect from specified MAC devices that are identified in the device records.

  When you specify a group directory subtree during LDAP configuration in the ACS user interface, you enter the name assigned to the group directory subtree in your LDAP schema in the Group Directory Subtree text box.

How the LDAP User Groups Work

Each LDAP user group record sets up an LDAP user group that maps users connecting through one or more devices to the specified group.

For example, the LDAP user group identified as `cn=Group_1_colon` sets up an LDAP user group that will map users connecting from the host at 10.56.60.100 as well as from two other hosts:

```
dn: cn=Group_1_colon,ou=MAC Groups, ou=MAB Segment, o=mycorp
objectClass: top
objectClass: groupofuniquenames
description: group of delimited MAC Addresses
uniqueMember: cn=user00-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
uniqueMember: cn=user77a-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment
 , o=mycorp
uniqueMember: cn=user88-wxp.emea.mycorp.com, ou=MAC Addresses, ou=MAB Segment,
  o=mycorp
cn: Group_1_colon
```

ACS queries the LDAP database to determine to which user groups to assign users who connect from a host with a specified MAC address. ACS then assign users in the LDAP user group to a specified ACS user group that you configure.

Table 6-1 describes the attributes of the sample LDAP groups.

Table 6-1 Attributes in LDAP User Groups for Agentless Host Support

Attribute Name	Description
objectClass	The value in the example indicates that this is a "group of unique names." The value that you specify here must match the name that you specify in the Group Object Class text box when you specify the Common LDAP configuration during ACS LDAP configuration. For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 6-10.
uniqueMember	The value in the example is uniqueMember. One or more uniqueMember entries are used to specify one or more device type records that have been set up in the LDAP schema to define agentless hosts with specified MAC addresses. The objectClass field in the LDAP user group shown in the previous code sample includes user00, user77a, and user88. The name that you give to this field in your LDAP schema must match the value that you enter in the Group Attribute Name text box when you specify the common LDAP configuration during ACS LD configuration. For information on configuring LDAP, see Configure an External LDAP Database for MAB Support, page 6-10.

Create One or More LDAP Database Configurations in ACS

After you have configured one or more LDAP databases to support MAB, configure ACS to query the LDAP databases.

The settings in the following procedure are based on the LDAP schema described in the previous section, Configure an External LDAP Database for MAB Support, page 6-10. For your ACS installation, configure ACS based on the schema that you set up for your network.

To create a LDAP configuration in ACS:

Step 1 In the navigation bar, click **External User Databases**.

The External User Databases page opens.

Step 2 Click **Database Configuration**.

The External User Database Configuration page opens.

Step 3 Click **Generic LDAP**.

The Database Configuration Creation table appears. If an LDAP configuration exists, the External User Database Configuration table also appears.

Step 4 Do one of the following. If:

- There are no existing LDAP database configurations, click **Create New Configuration**.
- The External User Database table appears, click **Configure**.

Step 5 If you are creating a new LDAP configuration, enter the name of the new configuration for generic LDAP and then click **Submit**.

Step 6 Click **Configure**.

The Generic LDAP Configuration page appears and contains four sections:

- **Domain Filtering**—Use to configure domain filtering, which is an optional configuration setting.

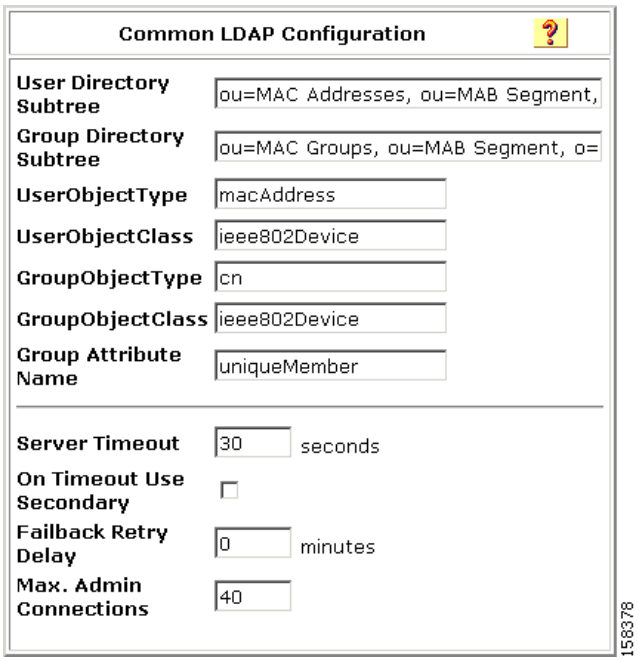
- **Common LDAP Configuration**—Configure the settings in this section to specify how ACS queries the LDAP database.
- **Primary LDAP Server**—Configure the settings in this section to specify the primary LDAP server.
- **Secondary LDAP Server**—Configure the settings in this section if you are setting up LDAP failback.

Step 7 If you want to set up Domain Filtering, refer to the "Configuring a Generic LDAP External User Database" section in Chapter 12 of the *User Guide for Cisco Secure Access Server 4.2*.

Step 8 Specify the common LDAP configuration

Figure 6-6 shows the Common LDAP Configuration section.

Figure 6-6 Common LDAP Configuration Section



You must specify:

- **User Directory Subtree**—Enter the distinguished name (DN) of the user directory subtree that contains all users. In MAB configuration, the users are, in effect, host devices.

  In the LDAP schema shown in Example 6-1, the DN of the User Directory Subtree is `ou=MAC Addresses, ou=MAB Segment, o=mycorp`.

- **Group Directory Subtree**—Enter the DN for the group directory subtree that contains all user groups as defined in your LDAP schema. In MAB configuration, the members of user groups are actually groups of MAC addresses.

  In the LDAP schema shown in Example 6-1, the DN of the group directory subtree is `ou=MAC Groups, ou=MAB Segment, o=cisco`.

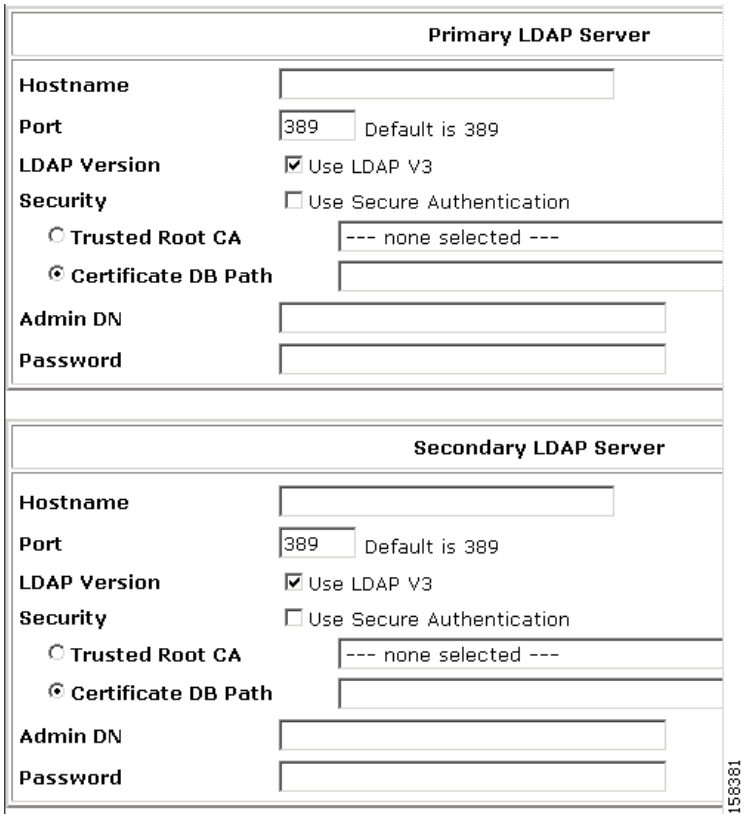
- **UserObjectType**— Enter the name of the user object type that is defined in your LDAP schema. In the LDAP schema shown in Example 6-1, the user object type is specified as `macAddress`.

- **UserObjectClass**—The value of the LDAP `objectType` attribute that identifies the record as a user. Often, user records have several values for the `objectType` attribute, some of which are unique to the user, some of which are shared with other object types. In the LDAP schema shown in Example 6-1, the user object class is specified as `ieee802Device`.
- **GroupObjectType**—The name of the attribute in the group record that contains the group name. In tIn the LDAP schema shown in Example 6-1, this is `cn`.
- **GroupObjectClass**—For MAB configuration, specify the name of a device record" that you have set up in your LDAP schema. For example, in Example 6-1, the group object class is `ieee802Device`.
- **GroupAttributeName**—For MAB configuration, specify the name of the LDAP attribute that specifies a LDAP user group. For example, in Example 6-1, each member of a LDAP user group is specified in a `uniqueMember` attribute.
  - **Server Timeout**—The number of seconds that ACS waits for a response from an LDAP server before determining that the connection with that server failed.
  - **On Timeout Use Secondary**—Determines whether ACS performs failover of LDAP authentication attempts.
  - **Failback Retry Delay**—The number of minutes after the primary LDAP server fails to authenticate a user that ACS resumes sending authentication requests to the primary LDAP server first. A value of zero (0) causes ACS to always use the primary LDAP server first.
  - **Max. Admin Connections**—The maximum number of concurrent connections (greater than zero (0)) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and Group Directory Subtree.

Specify LDAP server configuration information:

Figure 6-7 shows the Primary LDAP Server and Secondary LDAP Server configuration sections.

Figure 6-7 LDAP Server Configuration Sections



a. For the primary LDAP server specify:

- **Hostname**—The name or IP address of the server that is running the LDAP software. If you are using DNS on your network, you can type the hostname instead of the IP address.
- **Port**—The TCP/IP port number on which the LDAP server is listening. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information by viewing those properties on the LDAP server. If you want to use secure authentication, port 636 is the default.
- **LDAP Version**—ACS uses LDAP version 3 or version 2 to communicate with your LDAP database. If you check this check box, ACS uses LDAP version 3. If it is unchecked, ACS uses LDAP version 2.
- **Security—**ACS uses SSL to encrypt communication between ACS and the LDAP server. If you do not enable SSL, user credentials are passed to the LDAP server in clear text. If you select this option, then you must select **Trusted Root CA** or **Certificate Database Path**. ACS supports only server-side authentication for SSL communication with the LDAP server.

  ACS SE Only:

  You must ensure that the Port box contains the port number used for SSL on the LDAP server.
- **Trusted Root CA—**LDAP over SSL includes the option to authenticate by using the certificate database files other than the Netscape *cert7.db* file. This option uses the same mechanism as other SSL installations in the ACS environment. Select the certification authority that issued the server certificate that is installed on the LDAP server.
- **Certificate DB Path:** For ACS for Windows, this is the path to the Netscape *cert7.db* file For the ACS SE, this option provides a link to the Download Certificate Database page.

For detailed information on this field, refer to the "LDAP Configuration Options" section in Chapter 12 of the *User Guide for Cisco Secure Access Control Server*, "User Databases."

- **Admin DN**—The DN of the administrator; that is, the LDAP account which, if bound to, permits searches for all required users under the User Directory Subtree. It must contain the following information about your LDAP server:

  `uid=`*`user id`*`,[ou=`*`organizational unit`*`,][ou=`*`next organizational unit`*`]o=organization`

  where *`user id`* is the username, *`organizational unit`* is the last level of the tree, and *`next organizational unit`* is the next level up the tree.

  For example:

  ```
  uid=joesmith,ou=members,ou=administrators,o=cisco
  ```

  You can use anonymous credentials for the administrator username if the LDAP server is configured to make the group name attribute visible in searches by anonymous credentials. Otherwise, you must specify an administrator username that permits the group name attribute to be visible to searches.

Note If the administrator *username* that you specify does not have permission to see the *group name* attribute in searches, group mapping fails for users whom LDAP authenticates.

- **Password**—The password for the administrator account that you specified in the Admin DN box. The LDAP server determines case sensitivity.

b. If you want to set up LDAP server failback, then in the Secondary LDAP server section, specify information to identify the failback LDAP server.

The options and text input boxes in the Secondary LDAP Server section are the same as the ones in the Primary LDAP Server section.

Step 9 Click **Submit**.

Step 5: Configure User Groups for MAB Segments

During configuration of Network Access Profiles to enable agentless request processing, you will be required to map devices that have specified MAC addresses to one of the default user groups that ACS provides.

Before you assign the user groups, plan how to configure the user groups. For example, users associated with the user group can:

- Be denied access to the network
- Be limited by network access restrictions (NARs)
- Have specified password settings

For detailed information on how to set up user groups, refer to chapter 5 of the *User Guide for Cisco Secure ACS 4.2*, "User Group Management."

Step 6: Enable Agentless Request Processing

To enable agentless request processing, you must set up a Network Access Profile that enables the feature. To create a NAP to enable agentless request processing:

Step 1 Create a new NAP.

See Create a New NAP, page 6-18 for details.

Step 2 In the Protocols page, check the **Allow Agentless Request Processing** check box.

Step 3 In the Authentication section, configure MAB.

See Configure MAB, page 6-21 for details.

Step 4 If you are using agentless request processing in a NAC environment, configure posture validation for the NAP.

See Enable Agentless Request Processing for a NAP, page 6-20 for details.

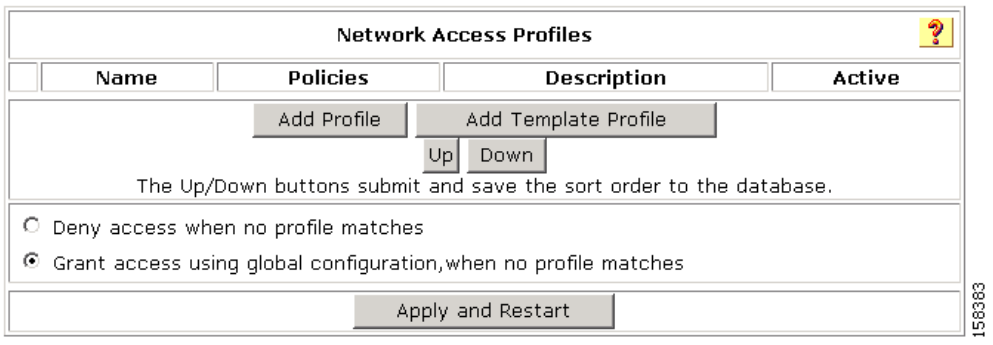
Create a New NAP

To create a new NAP:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens, as shown in Figure 6-8.

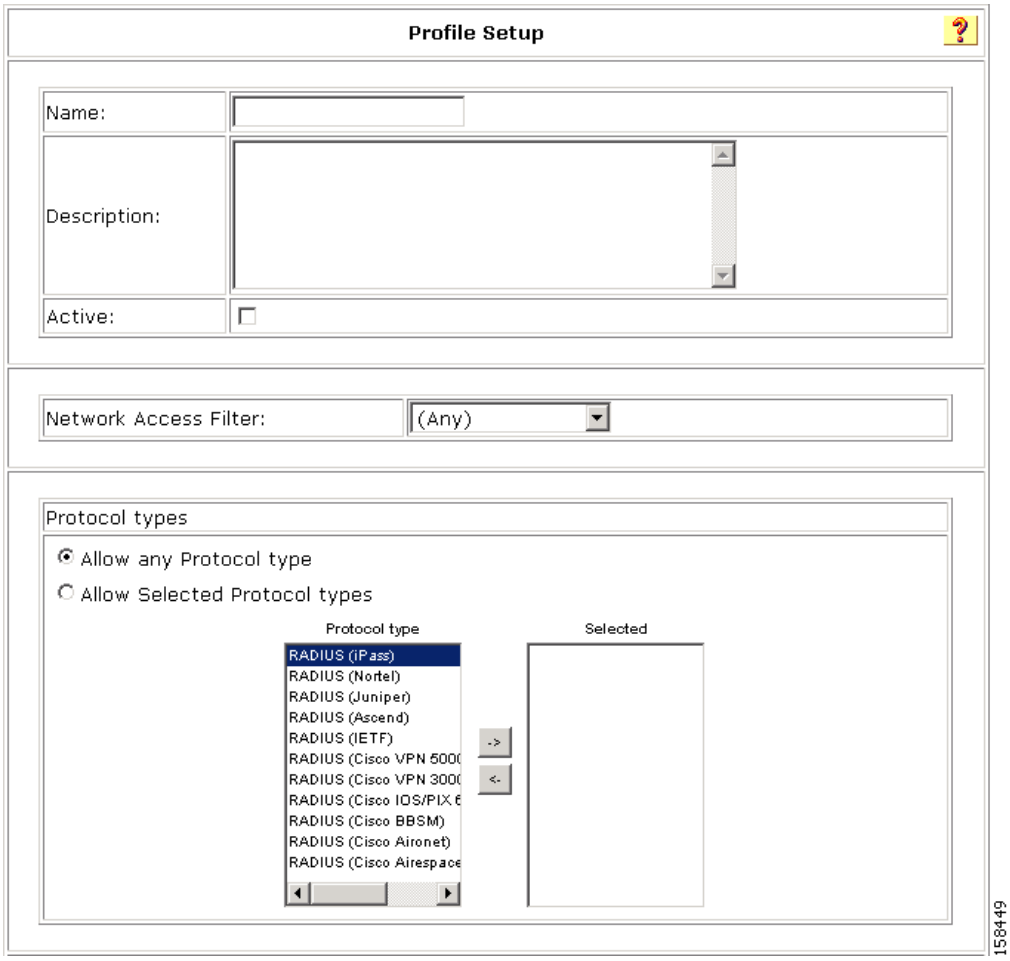
Figure 6-8 Network Access Profiles Page



Step 2 Click **Add Profile**,

The Profile Setup page opens, shown in Figure 6-9.

Figure 6-9 Profile Setup Page



Step 3 In the Name text box, enter the name of the NAP.

Step 4 If you have set up network access filters (NAFs) and want to apply one, then from the drop-down list of NAFs, choose the appropriate NAF.

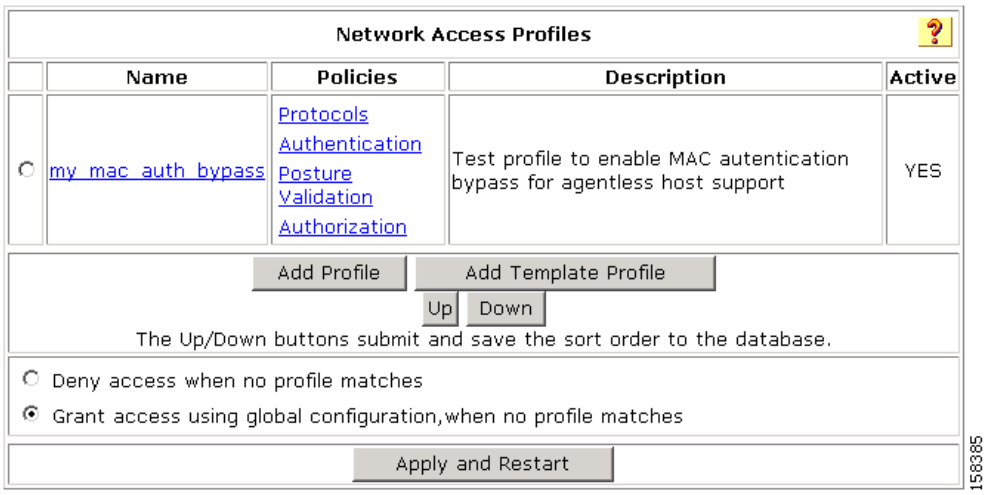
Step 5 In the Protocol types section, select at least one RADIUS protocol type.

Step 6 Configure additional NAP settings as required.

Step 7 Click **Submit**.

The Edit Network Access Protocols page for the new profile appears, as shown in Figure 6-10.

Figure 6-10 Edit Network Access Protocols Page



You are now ready to enable agentless request processing.

Enable Agentless Request Processing for a NAP

To enable agentless request processing for a NAP:

Step 1 In the Edit Network Access Profiles page, click **Protocols**.

The Protocols Settings page for the selected NAP opens. Figure 6-11 shows the top portion of the Protocols Settings page.

Figure 6-11 Protocols Settings Page

Step 2 Check the check box for A**llow Agentless Request Processing**.

Step 3 Configure additional protocol configuration options as required

Step 4 If you are using ACS in a NAC environment, check the **Allow Posture Validation** check box in the EAP Configuration area.

Step 5 Click **Submit**.

You are now ready to configure MAB settings.

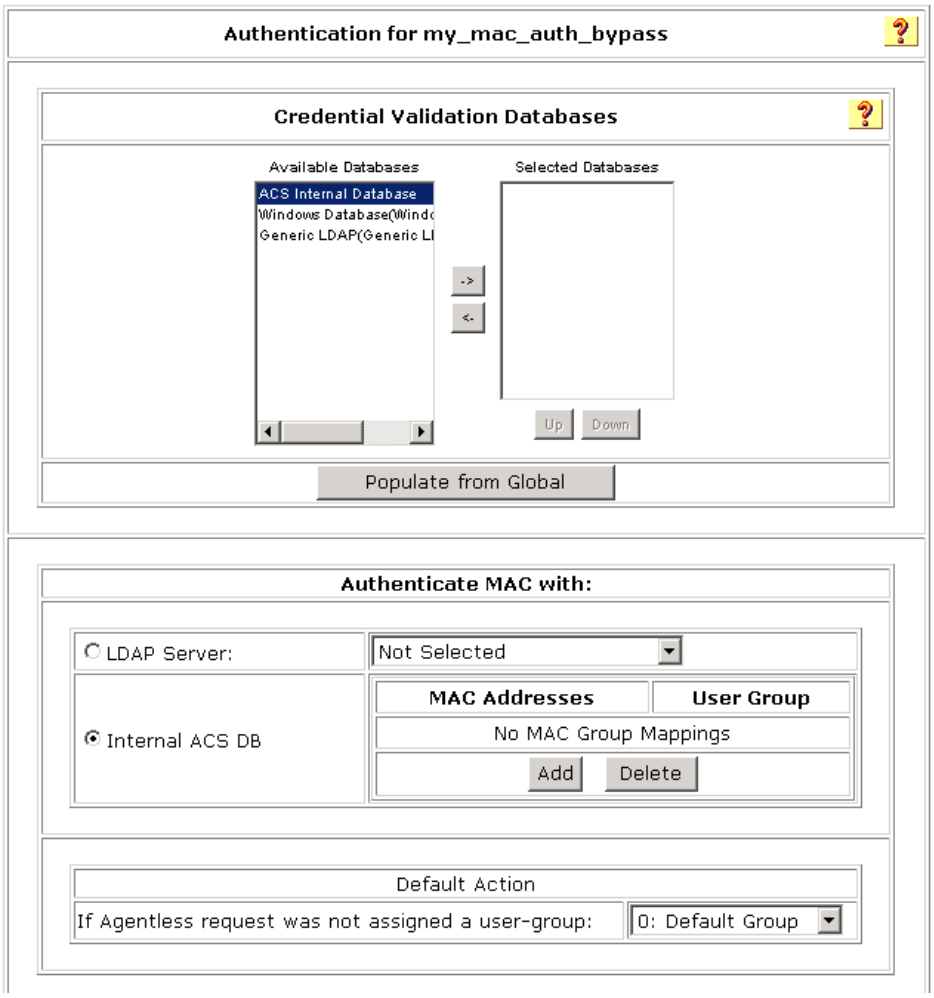
Configure MAB

To configure MAB:

Step 1 In the Edit Network Access Profiles page, click **Authentication**.

The Authentication page for the selected NAP opens. Figure 6-12 shows the Authentication Settings page.

Figure 6-12 Authentication Settings Page



Step 2 In the Credential Validation Databases section, choose the database(s) that ACS will use to authenticate agentless hosts.

Note If you clicked **Generic LDAP** or another LDAP database, choose **External User Databases** > **External User Database Configuration** and configure an LDAP database.

Step 3 If you specified an LDAP database in the Credential Validation Databases section, click **LDAP Server** and then select a LDAP database that you configured on the **External User Databases > External User Database Configuration** page.

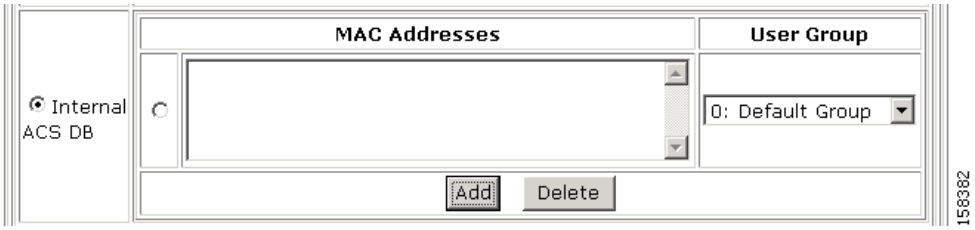
Step 4 If you will validate MAC addresses by using the ACS internal database:

a. Click **Internal ACS DB**.

b. Click **Add**.

A text box for entering MAC addresses and associated user group mappings appears, as shown in Figure 6-13.

Figure 6-13 MAC Address Input Area



c. In the MAC addresses input area, enter one or more MAC addresses to use in authenticating agentless hosts.

You can enter the MAC address in the following formats for representing MAC-48 addresses in human-readable form:

- Six groups of two hexadecimal digits, separated by hyphens (-) in transmission order; for example, *01-23-45-67-89-ab*.
- Six groups of two separated by colons (:); for example, *01:23:45:67:89:ab*.
- Three groups of four hexadecimal digits separated by dots (.); for example, *0123.4567.89ab*.

d. From the drop-down list of user groups in the User Group area, choose a user group to which devices having one of the specified MAC address are mapped.

e. To add additional groups of MAC addresses, click **Add** and enter additional groups and associated user groups as required.

Step 5 In the Default Action (If Agentless request was not assigned to a user group) area, from the drop-down list of user groups, choose a group to which to assign the MAC addresses if the MAC addresses are not found in the LDAP Server or the ACS Internal Database; or, if the LDAP Server is not reachable.

Step 6 If you enabled the EAP protocol and posture validation, set up posture validation rules in the Posture Validation section.

Step 7 As required, specify additional authorization rules in the Authorization section.

Step 8 Click **Submit**.

Step 7: Configure Logging and Reports

By default, the following information about MAB processing is logged to the *CSAuth* log file:

- The start of MAB request handling and what trigger is used to initiate MAB.

  The format of this message is:

  `Performing Mac Authentication Bypass on <MAC_address>`

  where *MAC_address* is the MAC address that triggered the processing.

- User group mapping actions that indicate which MAC address in the authentication database was mapped to what user group. The format of this message is:

  `<MAC_address> was (not) found in <DB_name> and mapped to <user_group> user-group`

  where *MAC_address* is the MAC address that was mapped, *DB_name* is the name of the database that was used to match the MAC_address, and *user_group* is the name of the user group to which the MAC address was mapped.

Note Because the results of MAC address lookup can influence the response that ACS returns to the NAD, the success or failure of the MAC address lookup has an effect on the user group that is mapped to an access request. Therefore, the MAC address lookup result might be listed in the Passed Authentications or Failed attempts report.

Configuring Reports for MAB Processing

When you configure reports, you can add a new attribute called `Bypass info` to the Passed Authentications and Failed Attempts reports.

To add this attribute:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Logging**.

The Logging Configuration page opens.

The Logging Configuration page shows three columns of ACS reports: CSV, ODBC, and syslog.

Step 3 To add the Bypass attribute to a specified report:

a. Click **Configure** under the report type for one of the reports that you want to modify; for example, click the CSV report for the Passed Authentications report.

   The Enable Logging page for the specified report opens.

b. Check the check box in the Enable Logging section.

c. In the Attributes column of the Select Columns to Log section, select the **Bypass Info** attribute.

d. Click the right arrow icon to move this attributed to the Logged Attributes column.

e. Select any other attributes that you want to log.

f. Set the other values on the Logging Configuration page as required.

g. Click **Submit**.

Step 4 Repeat Step 3 for additional report types as required.

Step 5 Repeat Steps 3 and 4 for the Failed Attempts report.

Configuration Steps for Audit Server Support

If you are using ACS with the NAC solution or with other applications that support the use of audit servers, you can set up agentless host support that uses an audit server.

An audit server runs a database that can enable further authentication of the information that is used to assign agentless host devices to user groups. For example, the categorization of devices in the LDAP schema might set up device categories such as *printer*, *PC*, or *FAX machine*. The database on the audit server can check whether a device with a specified MAC address or IP address is the type of device associated in the database with the specified MAC address or IP address. If it is not the correct device type, a specified authentication policy can be executed.

The mechanism that ACS 4.2 uses to communicate with audit servers in a NAC environment is called GAME group feedback. The GAME protocol defines the GAME groups. When you configure GAME group feedback for an audit server that is used in a NAP, you can enable the Request Device Type from Audit Server feature. If this feature is enabled, the audit feature can request a device type from the audit server and then check the device type against the device type that MAC authentication returns.

Configure GAME Group Feedback

To configure GAME group feedback:

Step 1 Import an audit vendor file by using **CSUtil**.

Step 2 Import a device-type attribute file by using **CSUtil**.

Step 3 Import NAC attribute-value pairs.

Step 4 Enable Posture Validation.

Step 5 In the External Posture Validation Audit Server Setup page, configure an external audit server.

Step 6 Enable GAME group feedback.

Step 7 In the external audit server posture validation setup section, configure:

- Which hosts are audited section.
- GAME group feedback.
- Device-type retrieval and mapping for vendors who have a device attribute in the RADIUS dictionary.

Step 8 Set up a device group policy.

The detailed steps for configuring GAME group feedback are described in Enable GAME Group Feedback, page 7-46 in Chapter 9, “NAC Configuration Scenario.”

CHAPTER 7

PEAP/EAP-TLS Configuration Scenario

You can select EAP-TLS as an inner method that is used within the tunnel that ACS establishes for PEAP authentication. If you select EAP-TLS, ACS can use it not only to encrypt the initial data sent through the PEAP protocol; but, once a secure tunnel is established between ACS and the NAD, to encrypt (for a second time) the data that is transmitted within the secure tunnel.

This enhanced encryption method greatly enhances the security of communications between ACS and the NAD.

Most customers who will use this feature are customers who use Microsoft supplicants.

Summary of Configuration Steps

To configure PEAP-TLS:

Step 1 Configure security certificates.

See Step 1: Configure Security Certificates, page 7-1 for details.

Step 2 Configure global authentication settings.

See Step 2: Configure Global Authentication Settings, page 7-5 for details.

Step 3 Specify EAP-TLS options.

See Step 3: Specify EAP-TLS Options, page 7-6 for details.

The following sections provide more details about the previous steps.

Step 1: Configure Security Certificates

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates and for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, "Advanced Configuration: Authentication and Certificates."

Obtain Certificates and Copy Them to the ACS Host

To use EAP-TLS, you must obtain and install security certificates.

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\Certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

`mkdir <`*`selected_drive`***`>:\Certs`**

where *`selected_drive`* is the currently selected drive.

Step 3 Copy the following files to the *\Certs* directory:

- *server.cer* (server certificate)
- *server.pvk* (server certificate private key)
- *ca.cer* (CA certificate)

Run the Windows Certificate Import Wizard to Install the Certificate

To run the Windows Certificate Import wizard to install the certificate on the server:

Step 1 Start Windows Explorer.

Step 2 Go to <*selected_drive*>:*Certs*.

where *`selected_drive`* is the currently selected drive.

Step 3 Double-click the *\Certs\ca.cer* file.

The Certificate dialog appears.

Step 4 Select **Install Certificate.**

The Windows Certificate Import wizard starts.

Step 5 To install the certificate, follow the instructions that the wizard displays.

Step 6 Accept the default options for the wizard.

Note Only perform this process once on a Windows 2000 Server.

Enable Security Certificates on the ACS Installation

To enable security certificates:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, shown in Figure 7-1.

Figure 7-1 Install ACS Certificate Page

Step 5 Ensure that you click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example `c:\Certs\server.cer`.

Step 7 In the Private Key File text box, type the server certificate private key location (path and name); for example: `c:\Certs\server.pvk`.

Step 8 In the Private Key password text box, type `1111`.

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Do not restart the services at this time.

Restart the services later, after you have completed the steps for adding a trusted certificate. See Add a Trusted Certificate, page 7-4.

Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, shown in Figure 7-2.

Figure 7-2 ACS Certification Authority Setup Page

Step 3 In the CA certificate file box, type the CA certificate location (path and name). For example: `c:\Certs\ca.cer`.

Step 4 Click **Submit**.

Add a Trusted Certificate

After you add a server certificate and set up the certificate authority, install a trusted certificate.

To add a trusted certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List appears.

Step 2 Locate the trusted certificate that you want to install and check the check box next to the certificate name.

For example, find the **Stress** certificate and check the check box next to it.

Step 3 Click **Submit**.

Step 4 To restart ACS, choose **System Configuration > Service Control**, and then click and then click **Restart**.

Step 2: Configure Global Authentication Settings

To configure global authentication settings:

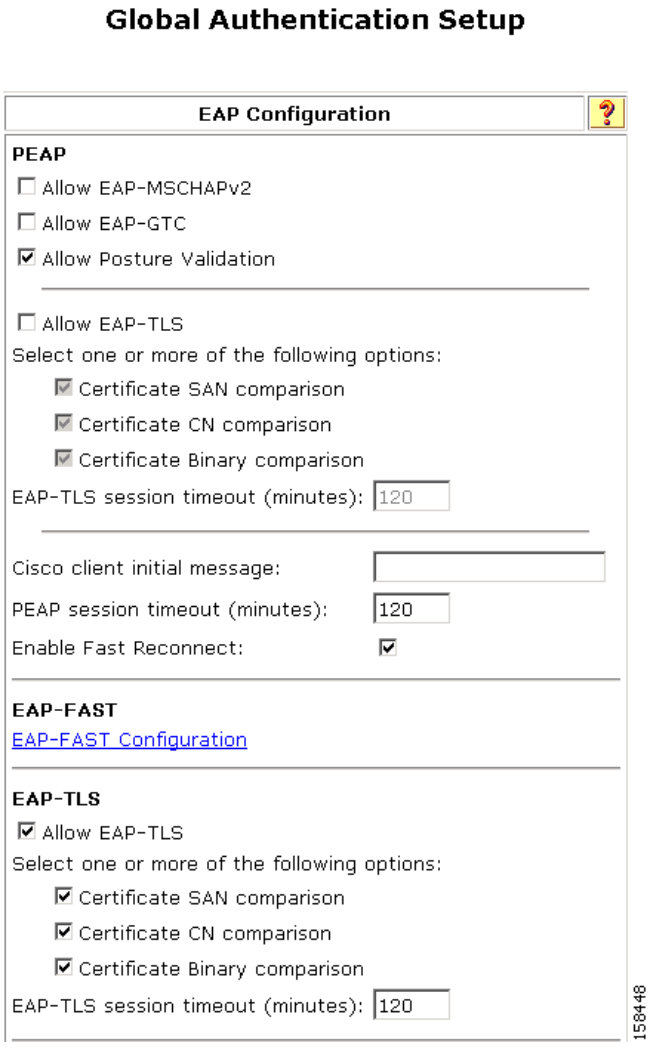
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup page opens, as shown in Figure 7-3.

Figure 7-3 Global Authentication Setup Page



Step 3 Specify the protocols to use with the PEAP protocol. They are:

- EAP_MSCHAP2
- EAP-GTC

Step 4 If you want to enable posture validation on this ACS installation, check the **Enable Posture Validation** check box.

Step 3: Specify EAP-TLS Options

Specify one or more of the certificate comparison options for EAP-TLS:

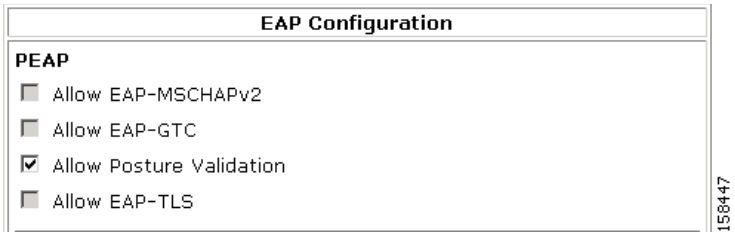
- **Certificate SAN Comparison**—Based on the name in the Subject Alternative Name (SAN) field in the user certificate.
- **Certificate CN Comparison**—Based on the name in the Subject Common Name (CN) field in the user certificate.
- **Certificate Binary Comparison**—Based on a binary comparison between the user certificate in the user object in the LDAP server or Active Directory and the certificate that the user presents during EAP-TLS authentication. You cannot use this comparison method to authenticate users in an ODBC external user database.

Step 4: (Optional) Configure Authentication Policy

You can enable EAP-TLS when you set up an authentication policy in the protocols section of Network Access Profile configuration.

Figure 7-4 shows the modified EAP configuration section on the NAP Protocols page.

Figure 7-4 EAP Configuration Section of NAP Protocols Page



CHAPTER 8

Syslog Logging Configuration Scenario

Overview

ACS provides a system logging (syslog) feature. With the addition of this feature, all AAA reports and audit report messages can be sent to up to two syslog servers.

Configuring Syslog Logging

To configure ACS to generate syslog messages:

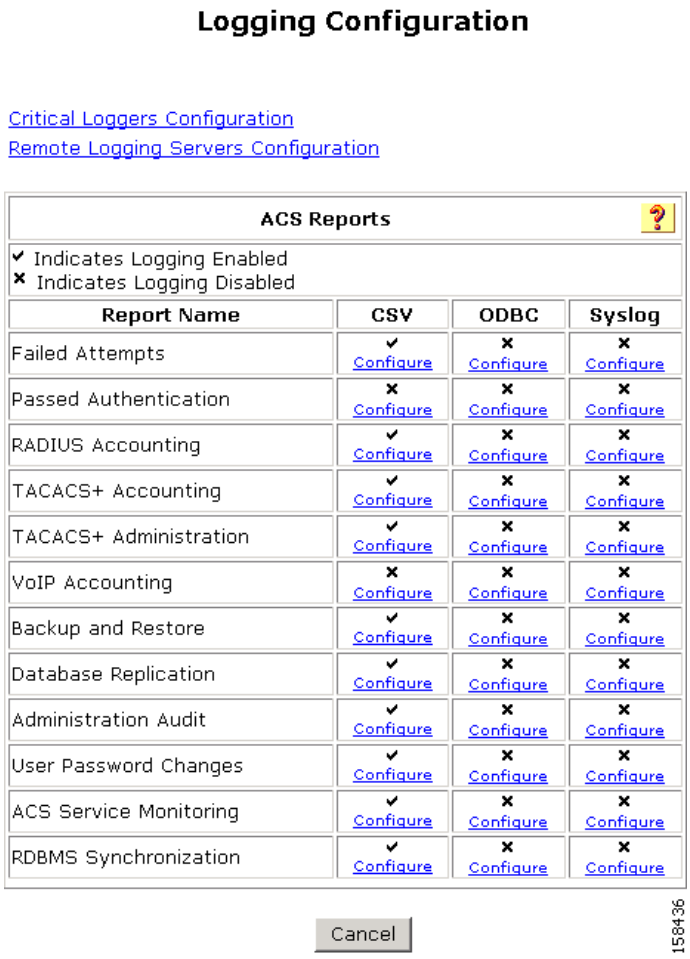
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Logging.**

The Logging page opens, shown in Figure 8-1.

Figure 8-1 Logging Configuration Page



Logging Configuration

Critical Loggers Configuration
Remote Logging Servers Configuration

ACS Reports

✔ Indicates Logging Enabled
✖ Indicates Logging Disabled

Report Name	CSV	ODBC	Syslog
Failed Attempts	✔ Configure	✖ Configure	✖ Configure
Passed Authentication	✖ Configure	✖ Configure	✖ Configure
RADIUS Accounting	✔ Configure	✖ Configure	✖ Configure
TACACS+ Accounting	✔ Configure	✖ Configure	✖ Configure
TACACS+ Administration	✔ Configure	✖ Configure	✖ Configure
VoIP Accounting	✖ Configure	✖ Configure	✖ Configure
Backup and Restore	✔ Configure	✖ Configure	✖ Configure
Database Replication	✔ Configure	✖ Configure	✖ Configure
Administration Audit	✔ Configure	✖ Configure	✖ Configure
User Password Changes	✔ Configure	✖ Configure	✖ Configure
ACS Service Monitoring	✔ Configure	✖ Configure	✖ Configure
RDBMS Synchronization	✔ Configure	✖ Configure	✖ Configure

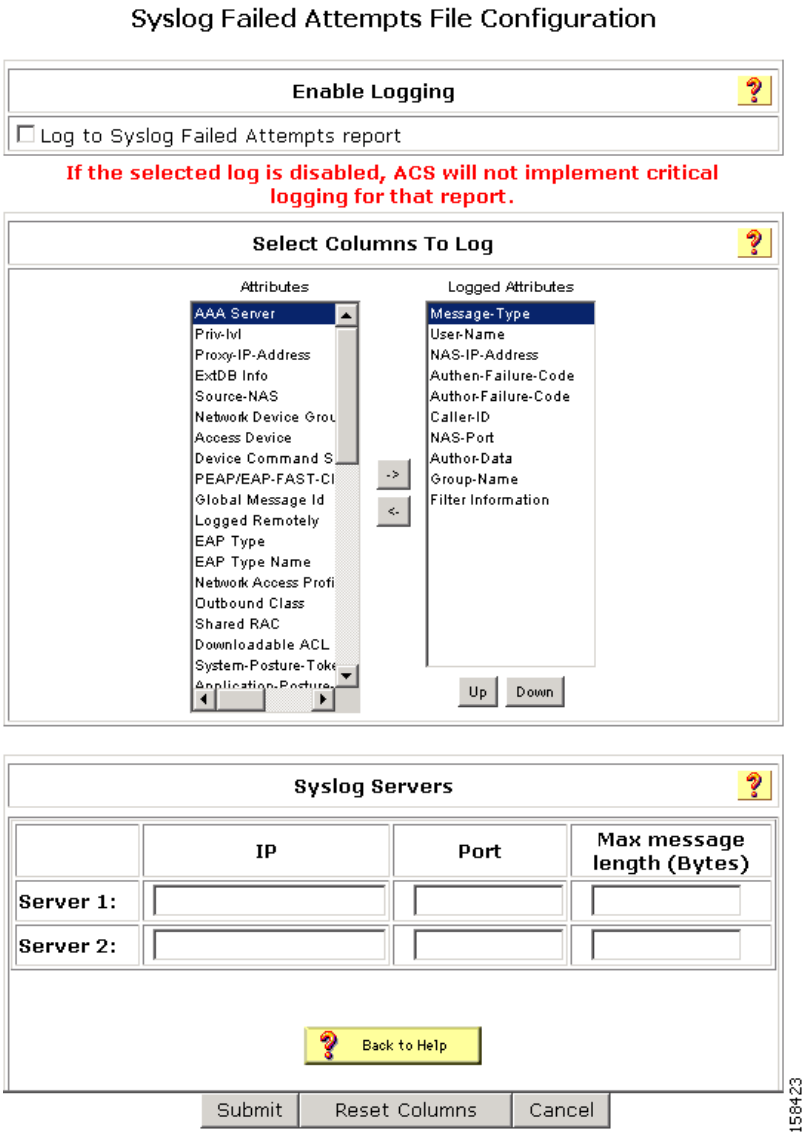
Cancel

158436

Step 3 To enable a syslog report, on the Logging Configuration page, click the **Configure** link in the syslog column, in the row for each report that you want to generate.

The Enable Login window for the specified report opens, as shown in Figure 8-2.

Figure 8-2 Enable Logging Page



Step 4 Check the check box for logging the specified information to syslog.

For example, in Figure 8-2, check the **Log to Syslog Failed Attempts Report** check box.

In the Select Columns to Log section, a list of the fields available for the specified syslog report appears.

Step 5 To move an attribute to the list of the attributes shown in the report, select the field in the Available column and then click the right arrow icon to move it to the Logged Attributes column.

In the Syslog Servers section, specify the following information for the syslog servers to which ACS will send logging information:

- **IP**—Enter the IP address of the syslog server.
- **Port**—Enter the syslog port number on the specified server.
- **Max message length (Bytes)**—Enter the maximum syslog message length that ACS will accept.

  You can enter information for up to two syslog servers.

Step 6 Click **Submit**.

Step 7 Repeat the process for any additional reports for which you want to enable syslog reporting.

Format of Syslog Messages in ACS Reports

Syslog messages included in ACS reports have the following format:

```
<n> mmm dd hh:mm:ss XX:XX:XX:XX TAG  msg_id total_seg seg# A1=V1
```

The elements of the message are:

- *n*—The Priority value of the message; it is a combination of facility and severity of the syslog message, which is calculated according to RFC 3164, by first multiplying the *facility* value by 8 and then adding the *severity* value.
- *mmm dd hh:mm:ss*—Date and time of the message.
- *XX:XX:XX:XX*—IP Address of the machine generating this syslog message.
- *TAG*—One of the following values, depending on the application name.
  - CisACS_01_PassedAuth—Cisco ACS passed authentications.
  - CisACS_02_FailedAuth—Cisco ACS failed attempts.
  - CisACS_03_RADIUSAcc—Cisco ACS RADIUS accounting.
  - CisACS_04_TACACSAcc—Cisco ACS TACACS+ accounting.
  - CisACS_05_TACACSAdmin—Cisco ACS TACACS+ administration.
  - CisACS_06_VoIPAcc—Cisco ACS VoIP accounting.
  - CisACS_11_BackRestore—ACS backup and restore log messages.
  - CisACS_12_Replication—ACS database replication log messages.
  - CisACS_13_AdminAudit—ACS administration audit log messages.
  - CisACS_14_PassChanges—ACS user password changes log messages.
  - CisACS_15_ServiceMon—ACS service monitoring log messages.
  - CisACS_16_ApplAdmin—ACS appliance administration audit log messages.
- *msg_id* —Unique message id. All segments of one message share the same message ID.
- *total_seg* —Total number of segments in this message.
- *seg#* -Segment sequence number within this message segmentation.
- *A1*=*V1*—Attribute-value pairs delimited by a comma (,) for Cisco ACS log messages and the message itself.

Facility Codes

ACS syslog messages use the following facility values:

- **4**—Security and authorization messages. This value is used for all AAA related messages (failed attempts, passed attempts, accounting, and so on).
- **13**—Log audit. This value is used for all other ACS report messages.

All ACS syslog messages use a severity value of 6 (informational).

For example, if the facility value is 13 and the severity value is 6, the Priority value is 110 ((8 x 13) + 6). The Priority value appears according to the syslog server setup, and might appear as

one of:

– **System3.Info**

– **<110>**

Note You cannot configure the format of the syslog facility and severity on ACS.

The following sample syslog message shows how the facility code and other information might look in an ACS-generated syslog message:

```
<110> Oct 16 08:58:07 64.103.114.149 CisACS_13_AdminAudit  18729fp11 1 0 AAA
Server=tfurman-w2k,admin-username=local_login,browser-ip=127.0.0.1,text-message=Administra
tion session finished,
```

In this example, <110 >represents the calculated value when the facility code is 13 (the log audit facility code).

Message Length Restrictions

When an ACS message exceeds the syslog standard length limitation or target length limitation, the message content is split into several segments:

- If all attribute-value elements fit into one segment then no segmentation is performed.
- If the message does not fit into one segment, the message is split between attribute-value pairs, keeping an attribute-value pair complete within the segment. That is, the first segment ends with a semicolon (;), while the next segment's content starts with the next attribute-value pair.
- In rare cases when one attribute-value pair is too long to fit in one segment all by itself, the value is segmented between sequenced segments of the message. Such segmentation might happen if attribute value contains several hundreds of characters. In general, ACS attribute values are designed to avoid such length.

All segments of one message have exactly the same header. The **<**msg_id**>** and **<**total_seg**>** values are shared between all segments. The **<**seg**#>** is set according to number of segments and the relative part of the content follows.

Use the following message length restrictions:

- For sending messages to a standard syslog server, the maximum message length should be 1024 bytes.
- For sending messages to Cisco Security Monitoring, Analysis and Response System (MARS), the maximum message length should be 500 bytes.
- Message segmentation should be used when the original message, including header and data, exceeds length limitations.

CHAPTER 9

NAC Configuration Scenario

This chapter describes how to set up Cisco Secure Access Control Server 4.2, hereafter referred to as ACS, to work in a Cisco Network Admission Control environment. This chapter contains the following sections:

Step 1: Install ACS

This section describes the installation process that you perform to run ACS, which runs on a Windows 2003 server or on a Cisco Secure ACS Solution Engine (ACS SE).

For detailed information on ACS installation, refer to the:

- *Installation Guide for Cisco Secure ACS for Windows Release 4.2*
- *Installation Guide for Cisco Secure ACS Solution Engine Release 4.2*

To install ACS:

Step 1 Start the ACS installation:

If you are installing ACS for Windows:

a. Using a local administrator account, log in to the computer on which you want to install ACS.

b. Insert the ACS CD into a CD-ROM drive on the computer.

c. If the CD-ROM drive supports the Windows autorun feature, the ACS for Windows dialog box appears; otherwise, run *setup.exe*, located in the root directory of the ACS CD.

d. In the Cisco Secure ACS for Windows dialog box, click **Install**.

If you are installing ACS SE, follow the instructions in the Installation Guide for Cisco Secure ACS Solution Engine 4.2. Chapter 2, "Installing and Configuring Cisco Secure ACS Solution Engine 4.2," provides detailed installation instructions.

During the installation process, you are prompted to enter a password for encrypting the internal database.

Step 2 Enter a password that is at least 8 characters long, and contains letters and numbers.

The ACS installation process for ACS for Windows automatically creates a shortcut to the ACS administrative GUI on your desktop.

Step 3 Double-click the icon to open a browser window to the ACS administrative GUI.

Step 4 If you do not see the icon on the desktop, open your browser from the machine on which you installed ACS and go to one of these addresses:

- http://*IP_address*:2002
- http://*hostname*:2002

where *IP_address* is the IP address of the host that is running ACS and *hostname* is the hostname of the host that is running ACS.

Step 2: Perform Network Configuration Tasks

This section describes:

Configure a RADIUS AAA Client

Before you can configure NAC support, you must configure a RADIUS AAA client.

To configure a RADIUS AAA client:

Step 1 In the navigation bar, click **Network Configuration**.

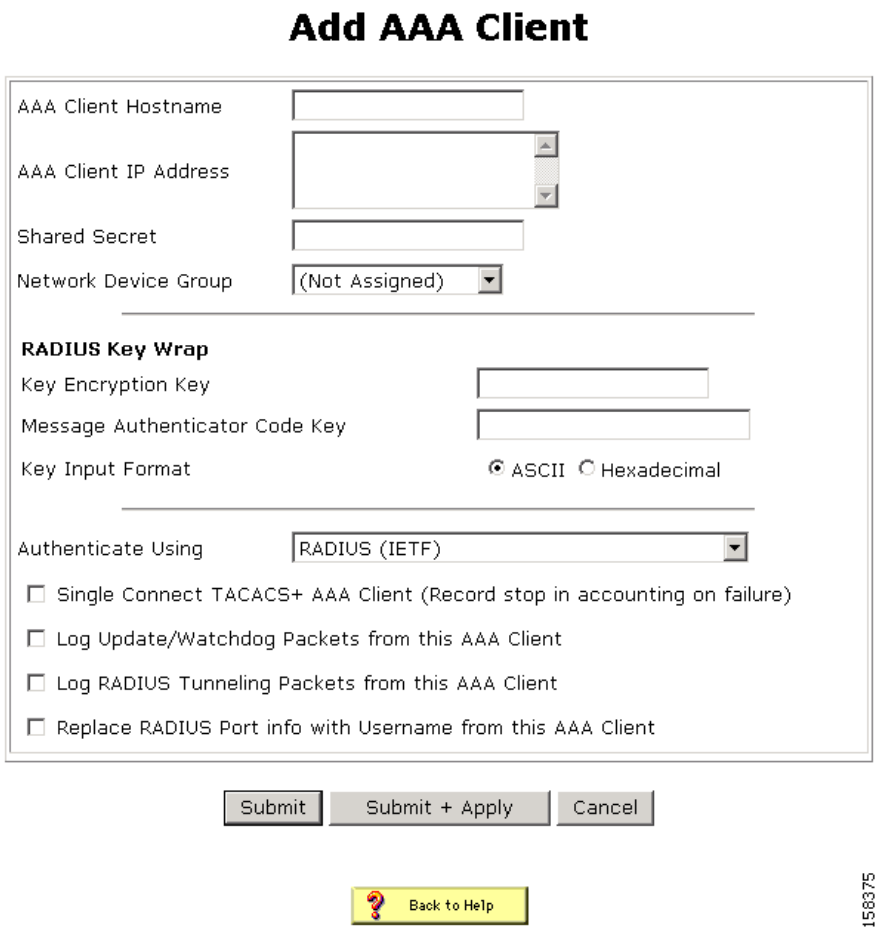
The Network Configuration page opens.

Step 2 Do one of the following:

- If you are using Network Device Groups (NDGs), click the name of the NDG to which you want to assign the AAA client. Then, click **Add Entry** below the AAA Clients table.
- To add AAA clients when you have not enabled NDGs, click **Not Assigned** and then click **Add Entry** below the AAA Clients table.

The Add AAA Client page opens, shown in Figure 9-1.

Figure 9-1 Add AAA Client Page



Step 3 In the AAA Client Hostname box, type the name assigned to this AAA client (up to 32 alphanumeric characters).

Step 4 In the AAA Client IP Address box, type the AAA client IP address or addresses.

Note You can define all network access devices (NADs) as a single AAA client by entering IP address wildcards; for example, *.*.*.*. Note however, that AAA client definitions with wildcards cannot overlap with other AAA client definitions, regardless of the authentication type configured for the AAA clients.

Step 5 In the Shared Secret box, type a shared secret key for the AAA client.

The shared secret is a string that you determine; for example, `mynet123`. The shared secret must be identical on the AAA client and ACS. Keys are case sensitive. If the shared secrets do not match, ACS discards all packets from the network device.

Step 6 If you are using NDGs, from the Network Device Group list, choose the name of the NDG to which this AAA client should belong, or, click **Not Assigned** to set this AAA client to be independent of NDGs.

Step 7 Type the shared secret keys for RADIUS Key Wrap in EAP-TLS authentications.

Each key must be unique, and must also be distinct from the RADIUS shared key. You can configure these shared keys for each AAA client, as well as for each NDG. The NDG key configuration overrides the AAA client configuration. If the key entry is null, ACS uses the AAA client key. You must enable the Key Wrap feature in the NAP Authentication Settings page to implement these shared keys in EAP-TLS authentication:

a. **Key Encryption Key (KEK)**—Used for encryption of the Pairwise Master Key (PMK). The maximum length is 20 characters.

b. **Message Authenticator Code Key (MACK)**—Used for the keyed hashed message authentication code (HMAC) calculation over the RADIUS message. The maximum length is 16 characters.

c. **Key Input Format**—Click the format of the key, ASCII or hexadecimal strings (the default is ASCII).

Step 8 From the Authenticate Using list, choose **RADIUS (IOS/PIX)**.

Step 9 Specify additional AAA client settings as required.

Step 10 Click **Submit + Apply**.

Configure the AAA Server

Your AAA server is automatically populated during the installation of ACS, using the hostname assigned to Windows 2003 system. You must specify some additional configuration information to enable the server to communicate with AAA clients.

To configure the AAA server:

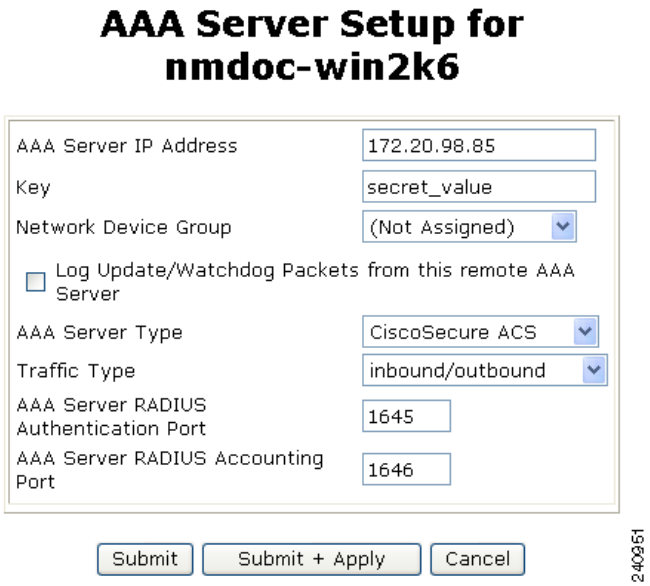
Step 1 In the navigation bar, click **Network Configuration**.

The Network Configuration page opens.

Step 2 In the AAA Servers table, click the name of the AAA server in the AAA Server Name column.

The AAA Server Setup page opens, shown in Figure 9-2.

Figure 9-2 AAA Server Setup Page



Step 3 In the Key field, enter the shared secret that you used to set up the AAA clients.

Step 4 Click **Submit and Apply**.

Step 3: Set Up System Configuration

This section describes the following tasks:

- Install and Set Up an ACS Security Certificate, page 9-5
- Set Up Global Configuration, page 9-8

Install and Set Up an ACS Security Certificate

You must configure ACS with a digital certificate for establishing client trust when ACS challenges the client for its credentials. Note these points:

- For authenticated in-band Protected Access Credential (PAC) provisioning for EAP-FAST, the client must have a certificate that matches the one installed in ACS.
- For the most scalable NAC environments, Cisco recommends a production public key infrastructure (PKI) that the production certificate authority (CA) or registration authorities (RAs) sign.

This section describes a simplified procedure for the ACS for Windows platform. For detailed information on installing certificates and for information on how to install certificates on the Cisco Secure ACS Solution Engine platform, see Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, "Advanced Configuration: Authentication and Certificates."

Obtain Certificates and Copy Them to the ACS Host

To copy a certificate to the ACS host:

Step 1 Obtain a security certificate.

Step 2 Create a *\certs* directory on the ACS server.

a. Open a DOS command window.

b. To create a certificates directory, enter:

```
mkdir <selected_drive>:\certs
```

where `selected_drive` is the currently selected drive.

Step 3 For example, copy the following files to the *\certs* directory:

- *ACS-1.nac.cisco.com.cer* (server certificate)
- *ACS-1.PrivateKey.txt* (server certificate private key)
- *ca.nac.cisco.com.cer* (CA certificate)

You are now ready to set up the ACS certification authority.

Set Up the ACS Certification Authority

To set up the ACS certification authority:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **ACS Certificate Setup.**

The ACS Certificate Setup page opens.

Step 3 Click **ACS Certification Authority Setup**.

The ACS Certificate Authority page opens, as shown in Figure 9-3.

Figure 9-3 ACS Certificate Authority Setup Page

Step 4 Enter the path and filename for the certificate authority certificate and then click **Submit**.

Step 5 Restart ACS.

To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.

Edit the Certificate Trust List

After you set up the ACS certification authority, you must add the CA certificate to the ACS Certificate Trust list.

To add the certificate to the Certificate Trust list:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Choose **ACS Certificate Setup > Edit Certificate Trust List**.

The Edit Certificate Trust List page opens.

Step 3 In the list of certificates, locate the CA certificate that you installed and check the check box next to it.

Step 4 Click **Submit**.

Step 5 Restart ACS.

To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.

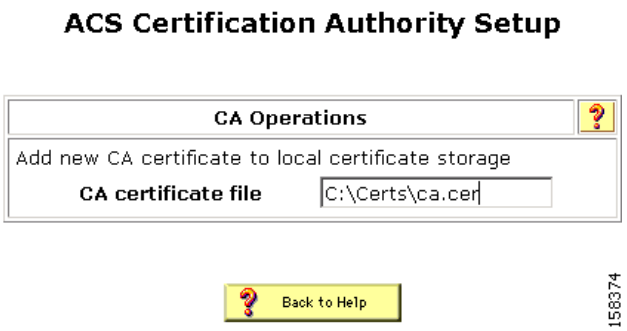
Install the CA Certificate

To install the CA Certificate:

Step 1 Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

Step 2 The ACS Certification Authority Setup page appears, as shown in Figure 9-4.

Figure 9-4 ACS Certification Authority Setup Page



Step 3 In the CA certificate file box, type the CA certificate location (path and name); for example: `c:\Certs\ca.cer`.

Step 4 Click **Submit**.

Install the ACS Certificate

To enable security certificates on the ACS installation:

Step 1 In the navigation bar, click **System Configuration**.

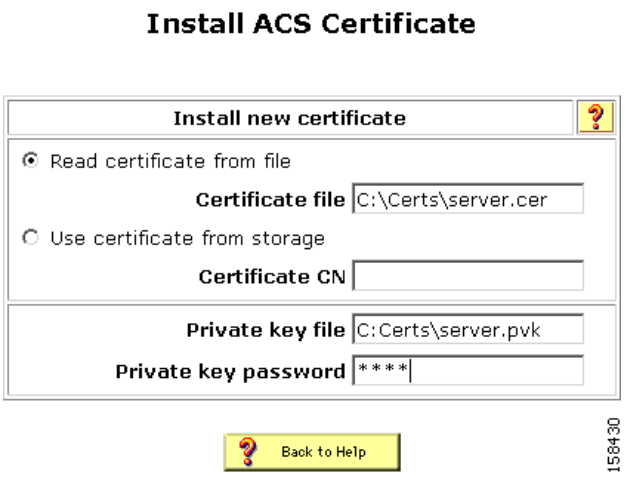
The System Configuration page opens.

Step 2 Click **ACS Certificate Setup**.

Step 3 Click **Install ACS Certificate**.

Step 4 The Install ACS Certificate page opens, as shown in Figure 9-5.

Figure 9-5 Install ACS Certificate Page



Step 5 Click the **Read certificate from file** radio button.

Step 6 In the Certificate file text box, enter the server certificate location (path and name); for example: **`c:\Certs\server.cer`**.

Step 7 In the Private key file text box, type the server certificate private key location (path and name); for example: **`c:\Certs\server.pvk`**.

Step 8 In the Private Key password text box, type the private key password; for example **`cisco123`.**

Step 9 Click **Submit.**

Step 10 ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.

Step 11 Restart ACS.

To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.

Set Up Global Configuration

This section describes the following tasks:

- Set Up Global Authentication, page 9-9
- Set Up EAP-FAST Configuration, page 9-12

Set Up Global Authentication

In the global authentication setup, you specify the protocols that ACS uses to transfer credentials from the host for authentication and authorization. Unless you have a limited deployment environment or specific security concerns, you should globally enable all protocols. If you do not enable the protocols in the global authorization setup, then they will not be available later in the Network Access Profiles configuration interface.

To set up global authentication:

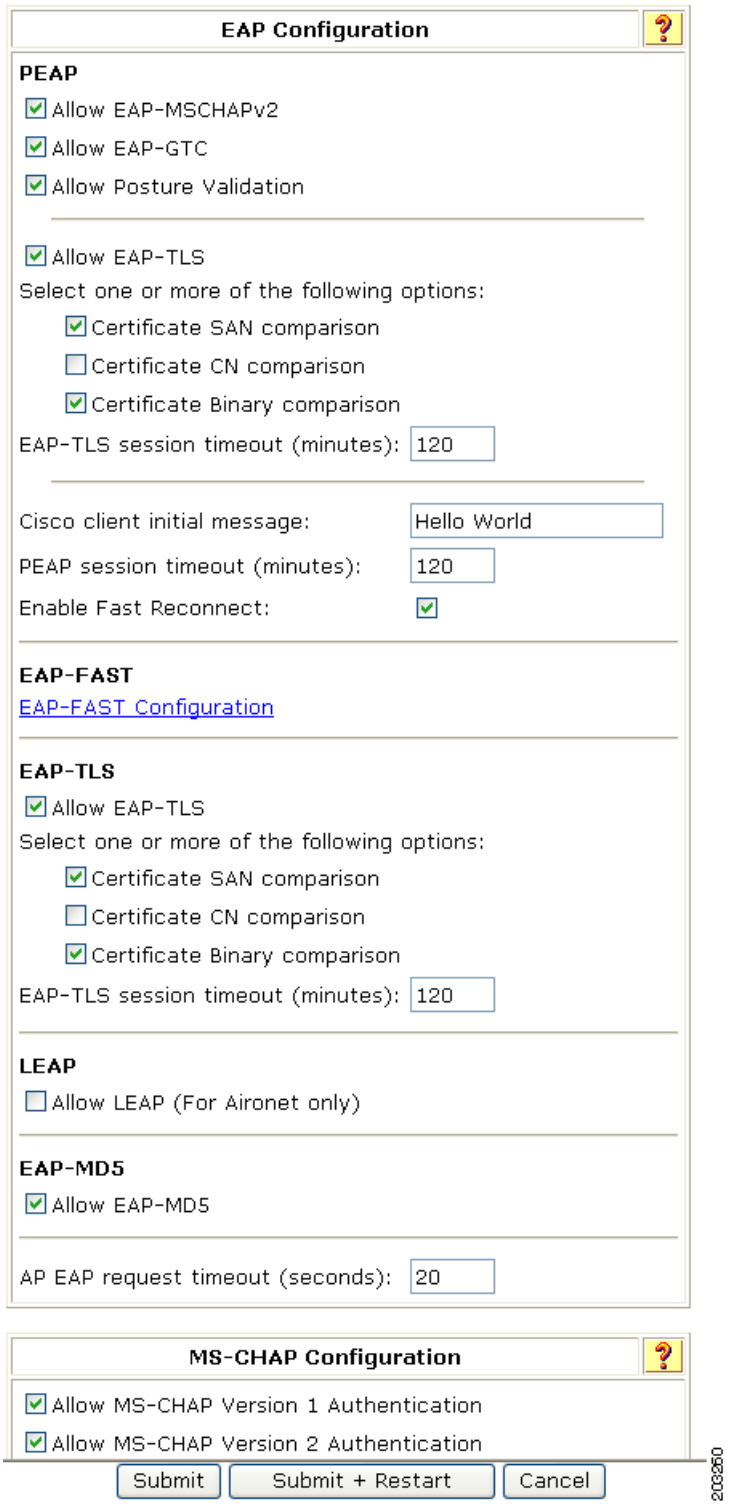
Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup Page appears, as shown in Figure 9-6.

Figure 9-6 Global Authentication Setup Page



Step 3 To make the PEAP global authentication parameters available in the NAP configuration, check the check boxes for:

- **Allow EAP-MSCHAPv2**.

  EAP-MSCHAP is a variation of the Microsoft Challenge and Response Protocol that is used with the Protected Extensible Access Protocol (PEAP). For a description of the EAP-MSCHAPv2 protocol, see the "Authentication" section in Chapter 1 of the *User Guide for Cisco Secure ACS, 4.2*, "Overview."

- **Allow EAP-GTC**.

  For a description of the EAP Generic Token Card (EAP-GTC) protocol, see "EAP-FAST Authentication" in Chapter 9 of the *User Guide for Cisco Secure ACS 4.2*, "System Configuration: Authentication and Certificates."

- **Allow Posture Validation**.

  For a description of Posture Validation, see the "What Is Posture Validation" section in Chapter 13 of the *User Guide for Cisco Secure ACS, 4.2*, "Posture Validation."

Step 4 In the EAP-TLS section:

a. Check the **Allow EAP-TLS** check box.

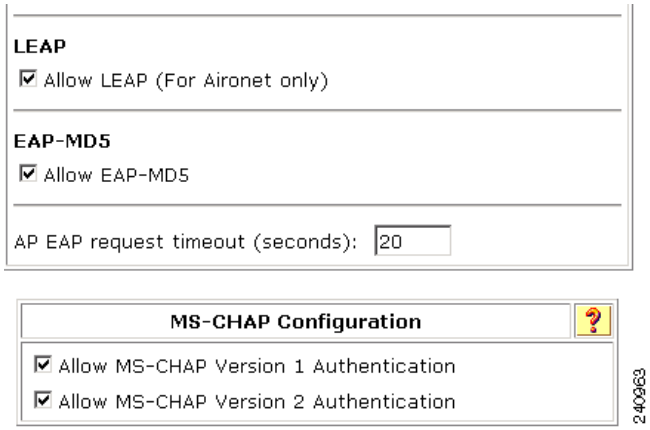
b. Check the **Certificate SAN comparison** and **Certificate Binary comparison** check boxes.

c. Leave the EAP-TLS timeout field set to the default (120 minutes).

Step 5 In the EAP-MD5 section, check the **Allow EAP-MD5** check box.

Step 6 Scroll down to the MS-CHAP configuration section, and check the **Allow MS-CHAP Version 1** Authentication and **Allow MS-CHAP Version 2** Authentication check boxes, as shown in Figure 9-7.

Figure 9-7 MS-CHAP Authentication Selection



Step 7 Click **Submit + Restart**.

Step 8 Go to Set Up EAP-FAST Configuration, page 9-12, and configure EAP-FAST authentication.

Set Up EAP-FAST Configuration

To configure ACS to work with NAC and use EAP-FAST with posture validation:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

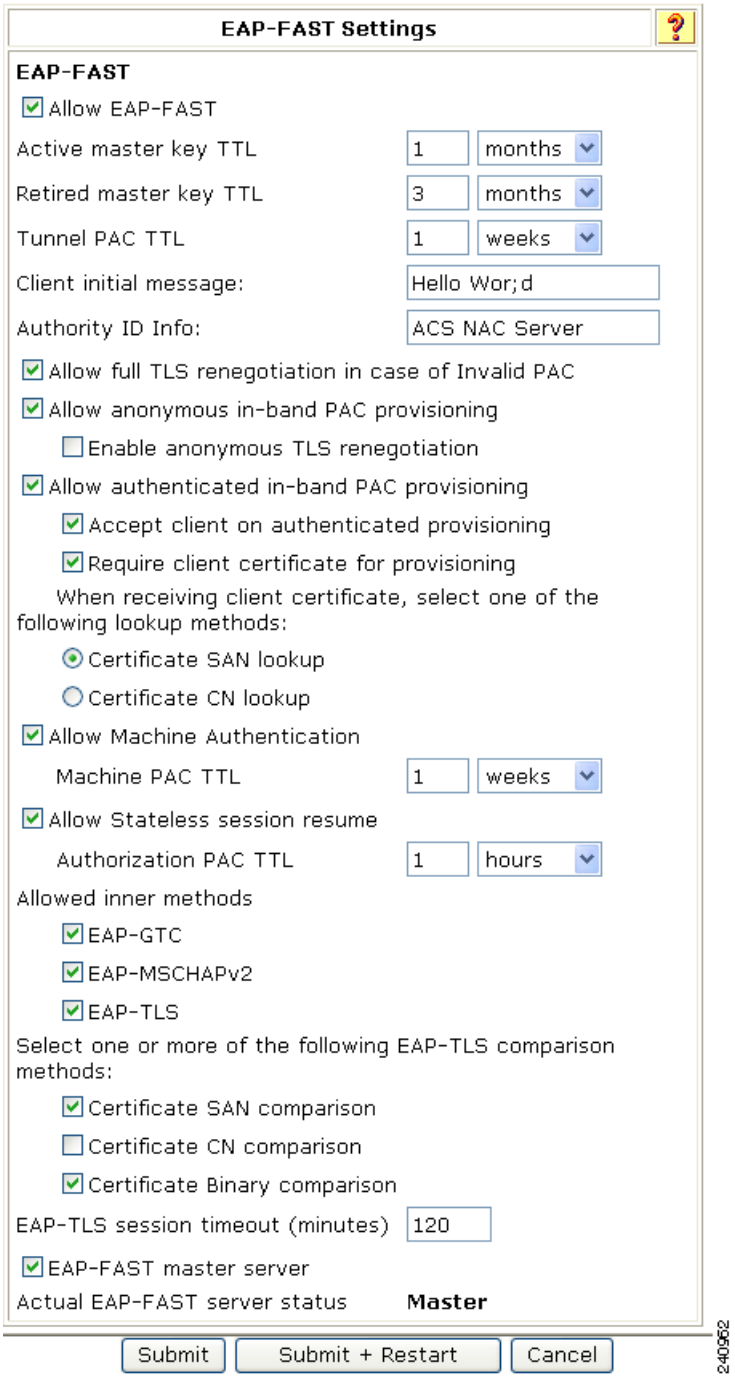
Step 2 Click **Global Authentication Setup**.

The Global Authentication Setup Page appears, as shown in Figure 9-6.

Step 3 Click **EAP-FAST Configuration**.

The EAP FAST Configuration page appears, as shown in Figure 9-8.

Figure 9-8 EAP-FAST Configuration Page



Step 4 Check the **Allow EAP-FAST** check box.

Step 5 In the Client Initial Message text box, enter a message; for example, **`Welcome`**.

Step 6 In the Authority ID Info field, enter the name of the certificate authority server. In the example shown in Figure 9-8, this is **`ACS NAC Server.`** However, this can be any string.

Step 7 Check the **Allow anonymous in-band PAC provisioning** and **authenticated in-band PAC provisioning** check boxes.

Step 8 Check the **Accept client on authenticated provisioning** and **Require client certificate for provisioning** check boxes.

Step 9 Check the check boxes for the **EAP-GTC**, **EAP-MSCHAPv2**, and **EAP-TLS** inner methods.

The **EAP-FAST Master Server** check box is automatically checked (enabled).

Check the **Certificate SAN** and **Certificate Binary comparison** check boxes to enable these EAP-TLS comparison methods.

Step 10 Click **Submit + Restart**.

Configure the Logging Level

To set ACS to full logging capabilities:

Step 1 In the navigation bar, click **System Configuration**.

The System Configuration page opens.

Step 2 Click **Service Control.**

Step 3 Under **Level of Detail,** click the **Full** radio button.

Note Setting the logging level to **Full** might affect system performance. Therefore, you should set the logging level to **Full** for an initial deployment when detailed troubleshooting is required. After the network has become stable, set the logging level to **Normal**.

Step 4 Check the **Manage Directory** check box and choose how many days of logging to keep. (Enter the number of days, based on how much space you have on your hard drive. Cisco recommends that you specify seven days.)

Step 5 Click **Restart** to restart ACS. (Wait until the browser's progress bar shows that the page has reloaded completely.)

Configure Logs and Reports

ACS logs records of users who gain or are refused network access, as well as records of other actions. You can output the information in the logs to reports that you view in the ACS GUI, which you can then save or print out and review. These reports summarize the logs, and provide useful information for debugging and tracking problems.

For detailed information on ACS logs and reports, see Chapter 10 of the *User Guide for Cisco Secure ACS. 4.2*, "Logs and Reports."

The Failed Attempts report and the RADIUS Accounting report are useful tools for monitoring the performance of the NAC/NAP network. And the Passed Authentications report is particularly useful in NAC-enabled networks; because, it shows the group mapping for each posture validation request. By default, the Passed Authentication report is unchecked (disabled).

To enable the Passed Authentications report:

Step 1 In the navigation bar, click **System Configuration**.

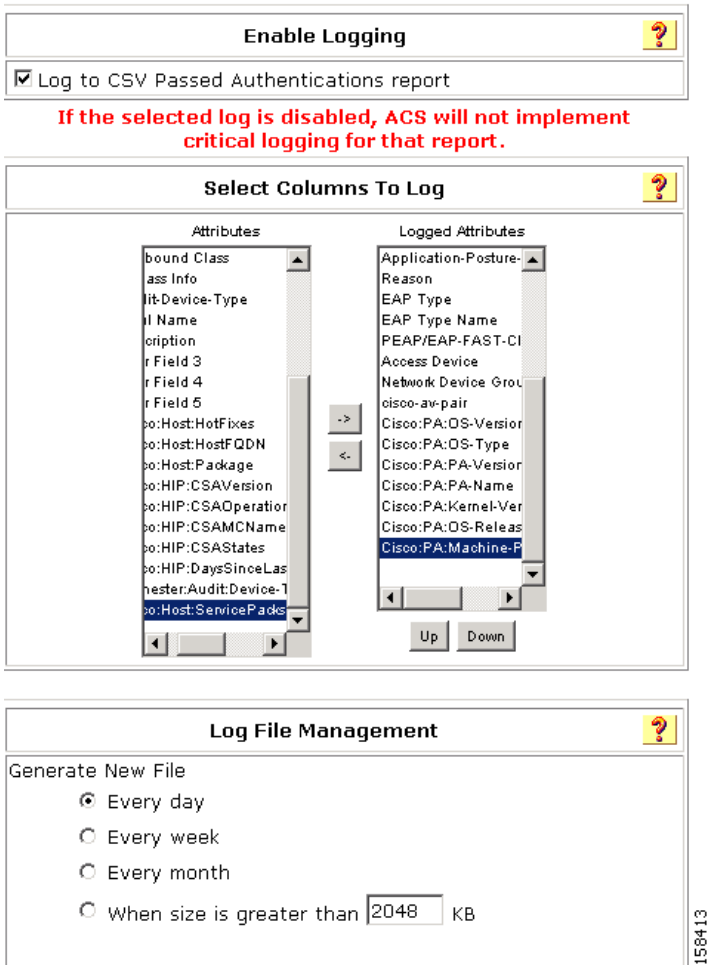
The System Configuration page opens.

Step 2 Click **Logging**.

The Logging Configuration page opens.

The CSV Passed Authentications File Configuration page opens, as shown in Figure 9-9.

Figure 9-9 CSV Passed Authentications File Configuration Page



Step 3 Check the **Log to CSV Passed Authentications Report** check box.

Step 4 Move the attributes that you want to log from the **Attributes** list to **Logged Attributes** list.

Some useful attributes to log are:

- Message-Type
- User-Name
- Caller-ID
- NAS-Port
- NAS-IP-Address
- AAA Server
- Filter Information
- Network Device Group
- Access Device
- PEAP/EAP-FAST-Clear-Name
- Logged Remotely
- EAP Type
- EAP Type Name
- Network Access Profile Name
- Outbound Class
- Shared RAC
- Downloadable ACL
- System-Posture-Token
- Application-Posture-Token
- Reason
- Profile Name
- Reason
- System-posture-token
- Application-posture-token

Step 5 Click **Submit.**

Step 6 In the ACS Reports table, click the **Configure** link for the CSV RADIUS Accounting report.

The CSV RADIUS Accounting File Configuration page appears.

Check the **Log to CSV RADIUS Accounting Report** check box.

Step 7 Move the attributes that you want to log from the Attributes list to the Logged Attributes list.

Some useful attributes to log are:

- User-Name
- Group-Name
- Calling-Station-Id
- Acct-Status-Type
- Acct-Session-Id
- Acct-Session-Time

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Packets
- Acct-Output-Packets
- Framed-IP-Address
- NAS-Port
- NAS-IP-Address
- Class
- Termination-Action
- Called-Station-Id
- Acct-Delay-Time
- Acct-Authentic
- Acct-Terminate-Cause
- Event-Timestamp
- NAS-Port-Type
- Port-Limit
- NAS-Port-Id
- AAA Server
- ExtDB Info
- Network Access Profile Name
- cisco-av-pair
- Access Device
- Logged Remotely

Step 8 Click **Submit.**

Step 4: Set Up Administration Control

This section describes how to add remote administrator access.

Add Remote Administrator Access

To prepare ACS for remote administration:

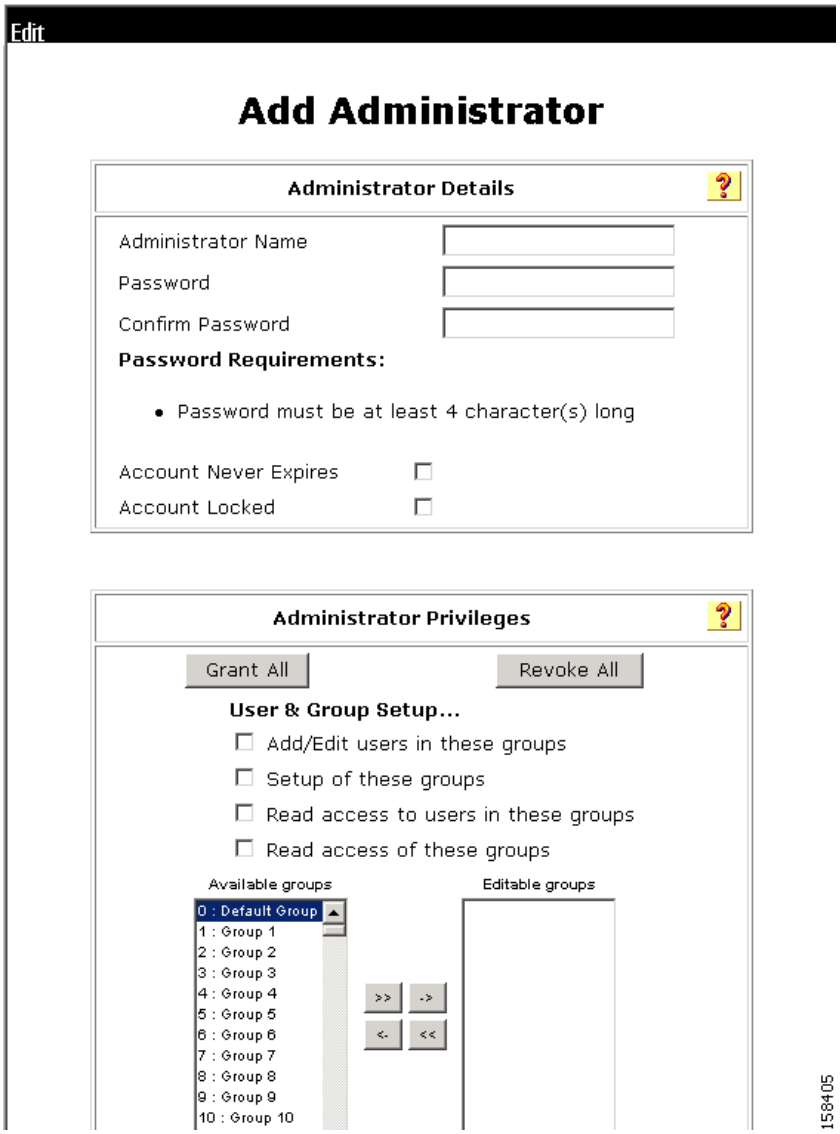
Step 1 In the navigation bar, click **Administration Control**.

The System Configuration page opens.

Step 2 Click **Add Administrator**.

The Add Administrator page opens, as shown in Figure 9-10.

Figure 9-10 Add Administrator Page



Step 3 In the Administrator Details area, specify the following information:

Option	Description
Administrator Name	Enter the login name for the ACS administrator account. Administrator names can contain 1 to 32 characters, but cannot contain the left angle bracket (<), the right angle bracket (>), or the backslash (\). An ACS administrator name does not have to match a network user name.
Password	Enter the password for the administrator to access the ACS web interface. The password can match the password that the administrator uses for dial-in authentication; or, it can be a different password. ACS enforces the options in the Password Validation Options section on the Administrator Password Policy page. Passwords must be at least 4 characters long and contain at least 1 numeric character. The password cannot include the username or the reverse username, must not match any of the previous 4 passwords, and must be in ASCII characters. If you make a password error, ACS displays the password criteria. If the password policy changes and the password does not change, the administrator remains logged in. ACS enforces the new password policy at the next login.
Confirm Password	Reenter the password that you entered in the password field.
Account Never Expires	If you want to override the lockout options set up on the Administrator Password Policy page (with the exception of manual lockout), check the check box next to Account Never Expires. If you check this option, the account never expires, but the password change policy remains in effect. The default value is unchecked (disabled).
Account Locked	If you want to lock out an administrator who is denied access due to the account policy options specified on the Password Policy page, check the **Account Locked** check box. When unchecked (disabled), this option unlocks an administrator who was locked out. Administrators who have the Administration Control privilege can use this option to manually lock out an account or reset locked accounts. The system displays a message that explains the reason for a lockout. When an administrator unlocks an account, ACS resets the Last Password Change and the Last Activity fields to the day on which the administrator unlocks the account. The reset of a locked account does not affect the configuration of the lockout and unlock mechanisms for failed attempts.

Step 4 Click **Grant All**.

This grants all privileges to the new administrator; or, specifies to which groups or actions this administrator is granted access.

Note For more information on administrative privileges, see the "Add Administrator and Edit Administrator Pages" section in Chapter 11 of the *User Guide for Cisco Secure Access Control Server 4.2*, "Administrators and Administrative Policy."

Step 5 Click **Submit**.

After performing these steps, from a remote host, you can open a browser in which to administer ACS.

The URLs for remote access are:

- http://*IP_address*:2002
- http://*hostname*:2002

Step 5: Set Up Shared Profile Components

Before you can set up NAPs, you must set up Shared Profile Components.

Shared Profile Components are configurations that can be reused across many different NAPs to set up filtering within ACS or to control network authorizations within RADIUS.

A NAP is a classification of network-access requests for applying a common policy. You can use NAPs to aggregate all policies that should be activated for a certain location in the network or for users who connect to the network by using specified protocols such as EAP over UDP (EoU) or 802.1x.

For detailed information on NAPs, see Chapter 14 of the *User Guide for Cisco Secure ACS, 4.2*, "Network Access Profiles."

This section describes the following tasks:

- Configure Network Access Filtering (Optional), page 9-20
- Configure Downloadable IP ACLs, page 9-21
- Configure Radius Authorization Components, page 9-25

Configure Network Access Filtering (Optional)

NAF is an ACS feature that groups several devices into one group. The devices can be ACS clients, ACS servers, ACS network device groups (NDGs), or a specific IP address. NAFs are particularly useful for defining NAPs.

When you set up Downloadable IP ACLs, you can:

- Assign the default NAF, which is **All AAA Clients**.

  This default allows access to all clients.
- Set up a NAF to limit access to specified clients.

To set up a NAF:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page opens.

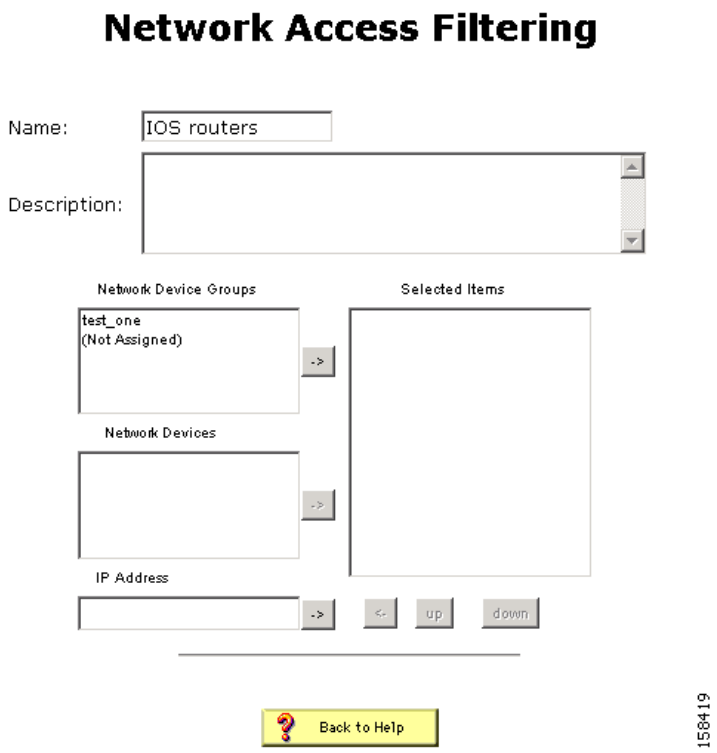
Step 2 Click **Network Access Filtering**.

The Network Access Filtering table appears. Initially, this table does not contain shared profile components.

Step 3 Click **Add**.

The Edit Network Access Filtering page opens, as shown in Figure 9-11.

Figure 9-11 Edit Network Access Filtering Page



Step 4 In the Name text box, enter a name for the network access filter.

Step 5 Move any devices or device groups to the Selected Items list.

To move a device or device group, select the item to move and then click the right arrow button to move it to the Selected Items list.

Step 6 Click **Submit**.

Configure Downloadable IP ACLs

Downloadable IP Access Control Lists (dACLs) are access lists that can be downloaded to enforce the network authorization of a host. Downloadable ACLs dynamically download Layer 3 and Layer 4 access control entries (ACEs) to a router; or, to a VPN concentrator and merge them with the default interface ACL.

In ACS 4.2, you can download access lists to specific devices or device groups.

You can define an access list that contains one or more dACLs and later download the list to network devices, based on their assignments to user groups. Before you define dACLs, enable dACLs.

Each Assessment Result (system posture token), according to its definition, should have its own ACL, which contains one or more Access Control Entries (ACEs) that will instruct the NAC network device (router) to block packets from going to a specific destination or allow packets to reach a specific destination.

To enable dACLs and NAFs, which are required to create NAPs:

- Add a new posture ACL.
- Add ACE entries for the ACL.
- Save the posture ACL.

Note These ACLs are referred to as posture ACLs because they are a component of a NAP that is used in posture validation.

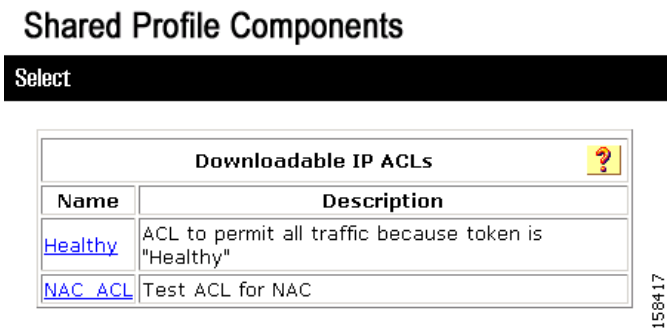
Adding an ACL

To add a new ACL:

Step 1 Choose **Shared Profile Components > Downloadable IP ACLs**.

A list of dACLs appears, as shown in Figure 9-12:

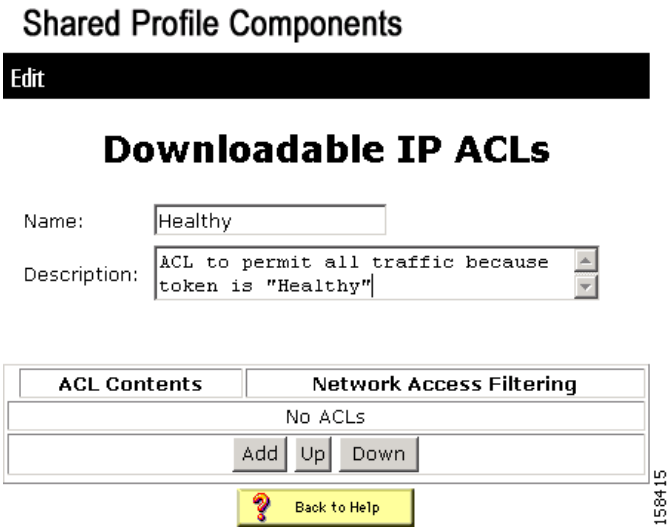
Figure 9-12 Downloadable IP ACL List



Step 2 Click **Add**.

The Edit Downloadable IP ACLs page opens, as shown in Figure 9-13.

Figure 9-13 Downloadable IP ACLs Page



Step 3 On the Downloadable IP ACLs page, enter a Name and optional Description for the ACL, as shown in Figure 9-13.

Note Do not use spaces in the name of the ACL. IOS does not accept ACL names that include spaces.

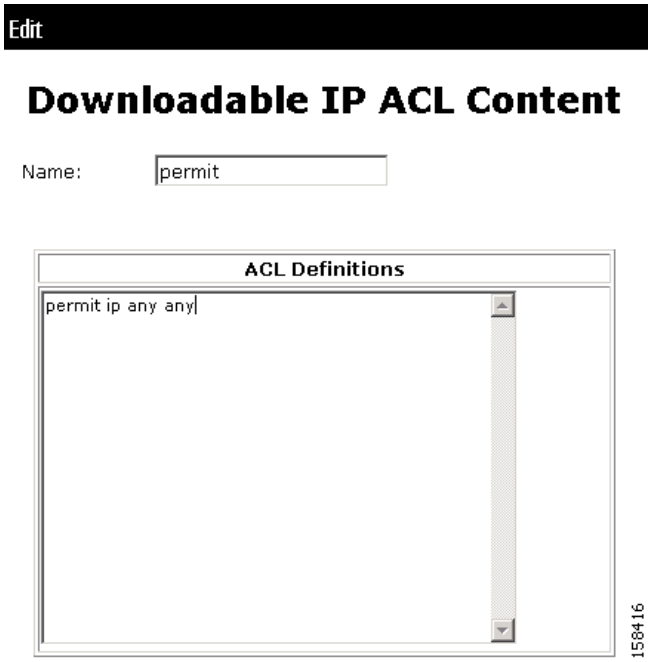
Adding an ACE

To add an ACE:

Step 1 On the Downloadable IP ACLs page, Click **Add** (below the ACL table of contents) to add a new ACE to the ACL and assign it to a NAF.

The Downloadable IP ACL Content page opens, as shown in Figure 9-14.

Figure 9-14 Downloadable IP ACL Content Page



Step 2 In the Name text box, type the ACL name.

Step 3 In the ACL Definitions input box, type definitions for the ACL.

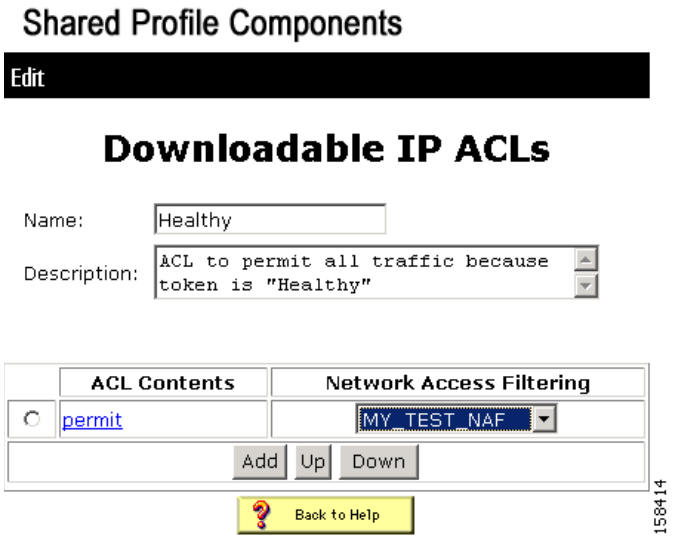
ACL definitions consist of a series of **permit** and **deny** statements that permit or deny access for specified hosts. For information on the syntax for ACL definitions, see the "Downloadable ACLs" section of Chapter 4 of the *User Guide for Cisco Secure Access Control Server 4.2*, "Shared Profile Components."

Step 4 Click **Submit**.

Note Before configuring the ACL on ACS, you should test the syntax on the device to ensure that each ACE is valid.

The Downloadable ACL page appears with the new ACL in the ACL Contents list, as shown in Figure 9-15.

Figure 9-15 Downloadable ACL Contents List with New Content



Step 5 From the drop-down list in the Network Access Filtering column of the ACL Contents table, choose the correct NAF for this ACL.

You can choose the default NAF (All AAA Clients), or you can specify a NAF that you have configured to control how access is set up for different devices or groups of devices.

For example, the syntax of an ACE on routers differs from the syntax on a Project Information Exchange (PIX) firewall. By using a NAF, you can assign the same ACL to a PIX and a router, even though the actual ACE that is downloaded is different.

Step 6 Click **Submit**.

The new ACL appears on the list of downloadable ACLs.

Saving the dACL

When you finish adding ACEs to the dACL, click **Submit** to save the dACL and submit it.

Configure Radius Authorization Components

Shared RADIUS Authorization Components (RACs) are sets of RADIUS attributes that ACS applies to Network Access Devices (NADs) during network authorization. Each RAC can contain one or more vendor RADIUS attributes, including Cisco IOS.PIX 6.0, IETF, and Ascend attributes.

By setting up RACs, you can dynamically assign RADIUS attributes to user sessions based on a policy. For example, you can create a RAC that gathers RADIUS attributes to define a VLAN. Users who access the network through a switch; for example, are then given access to specified VLANs based on how they are authorized and authenticated.

The sample RACs in this section provide RADIUS configurations to handle the most important services in the NAC environment:

- EoU (NAC L2 IP)
- NAC L2 802.1x

The sample RACs are:

- **Cisco_FullAccess—**Provides full access to the Cisco network. You use this RAC to grant access to clients that qualify as healthy.
- **Cisco_Restricted**—Provides restricted access to the Cisco network. You uses this RAC to grant partial (quarantined) access to clients that do not qualify as healthy.

To define RACs:

Step 1 In the navigation bar, click **Shared Profile Components**.

The Shared Profile Components page opens.

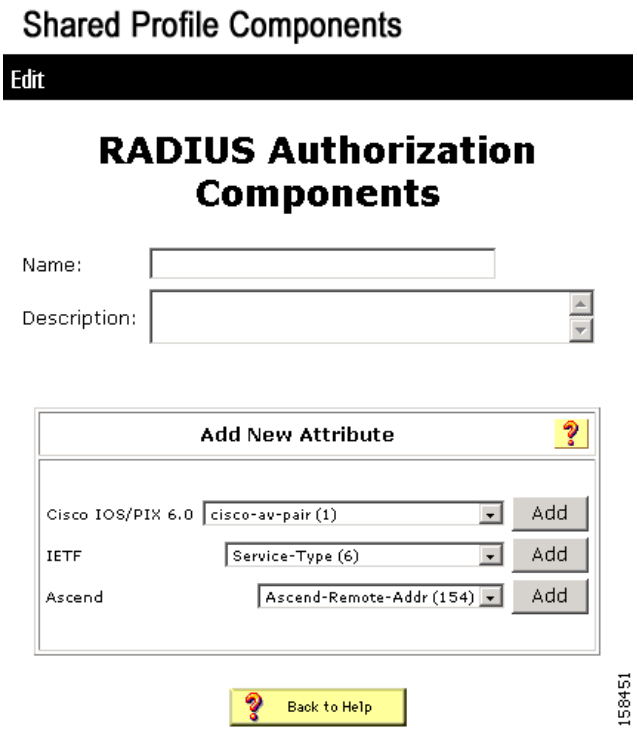
Step 2 Click **RADIUS Authorization Components**.

The RADIUS Authorization Components table appears. Initially, this table does not contain any RACs.

Step 3 Click **Add**.

The RADIUS Authorization Components Page opens, as shown in Figure 9-16.

Figure 9-16 RADIUS Authorization Components Page



Step 4 Enter a Name and Description in the RADIUS Authorization Components page.

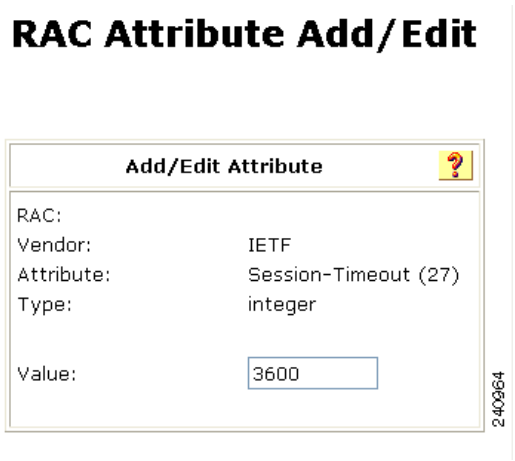
Step 5 In the Add New Attribute section, add the RADIUS attributes for the RAC.

a. To add an attribute, from the drop-down lists for Cisco IOS/PIX 6.0, IETF, and Ascend, choose the attribute that you want to add and then click **Add**.

For example, from the IETF drop-down list, choose **Session-Timeout (27)** and click **Add**.

The RAC Attribute Add/Edit page opens. Figure 9-17 shows the RAC Attribute Add/Edit page for **Session-Timeout (27)**.

Figure 9-17 RAC Attribute Add/Edit Page



b. In the Value field for the attribute, enter an appropriate value. Each attribute has specific value types based on how the attribute is defined.

   For example, for the **Session-Timeout (27)** attribute, enter a timeout value in seconds.

c. Click **Submit**.

Step 6 When you are finished adding attributes, click **Submit**.

Step 7 To enable the RAC, from the navigation bar, choose **System Configuration > Service Control** and then click **Restart**.

Figure 9-18 shows attribute selection for the Cisco_FullAccess RAC and Figure 9-19 shows attribute selection for the Cisco_Restricted RAC.

Figure 9-18 Attribute Selection for the Cisco_FullAccess RAC

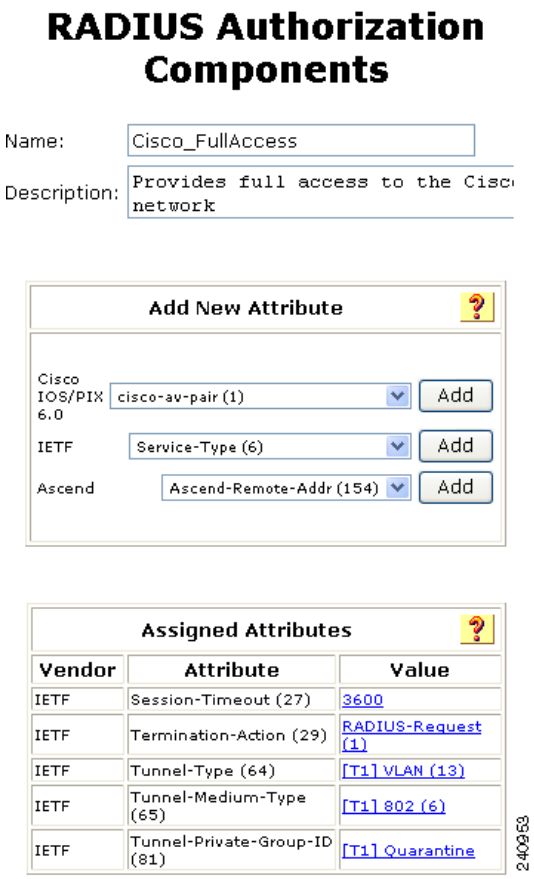
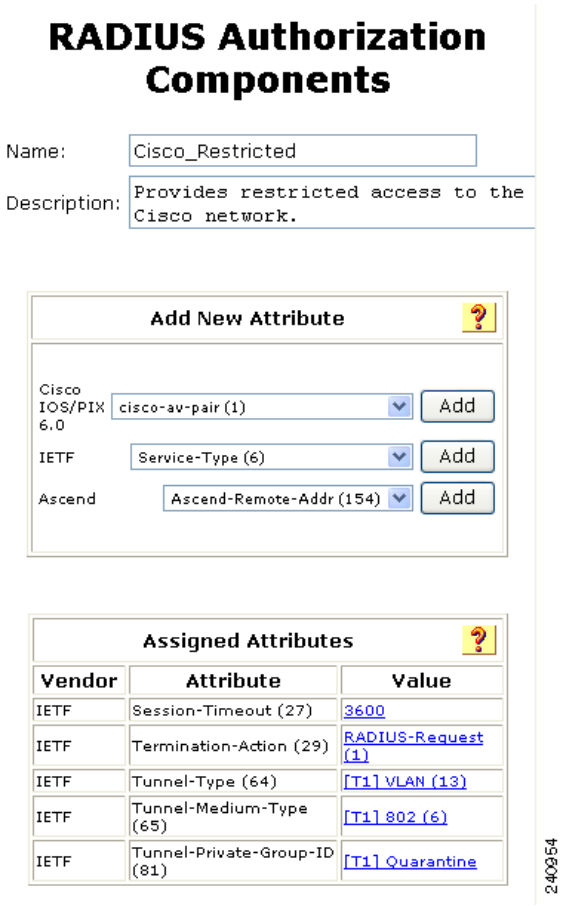


Figure 9-19 Attribute Selection for the Cisco_Restricted RAC



To enable VLAN assignment, the sample RACs include the following RADIUS attributes:

- **Session-Timeout (attribute 27)**—Enables a session timeout. In the sample RACs, the timeout value is set to 3600 seconds (six hours). Because session timeouts and revalidations use considerable network resources, you might want to set the timeout value to allow a longer timeout period; for example, 8 to 24 hours.
- **Termination-Action (attribute 29)**—Determines how the switch port responds to a session timeout. This attribute is only used in Access-Accept packets. When a session timeout occurs, the port drops all traffic on the switch until reauthentication is complete. In the sample RACs, this attribute is set to **RADIUS-Request (1)**. This ensures that the switch maintains the current VLAN assignment and network connectivity while reauthentication is in progress.
- **Tunnel-Type (attribute 64)**—Specifies the type of tunnel that is set up for the user to connect. In the sample RACs, this value is set to type 10, **VLAN**, which indicates that the user is granted access to a VLAN that is configured on the switch.

- **Tunnel-Medium-Type (attribute 65)**—Indicates which protocol to use over the tunnel. In the sample RACs, this is set to type 6, which specifies an 802 protocol. In the NAC/NAP environment, this is the 802.1x protocol.
- **Tunnel-Private-Group-ID (attribute 81**)—Indicates the group ID for the VLAN tunnel. In the sample RAC, this is set to **Quarantine**, which denotes a quarantine VLAN to which devices are assigned. In actual practice, you should set this value to a value that is configured on the switch.

For reference, Table 9-1 lists all of the possible attributes that ACS can send. An X in the NAC-L2-802.1x, NAC-L2-IP, or NAC-L3-IP column indicates that ACS can send the specified attribute in a RADIUS Accept-Response used with this technology.

Table 9-1 Attributes That Can Be Sent in the RADIUS-Accept Response

NAC-L2 -802.1x	NAC-L2-IP	NAC-L3-IP	Attribute Number	Attribute Name	Description
x			1	User-Name	Copied from EAP Identity Response in Access Request
	x	x	8	Framed-IP-Address	IP address of host
	x	x	26	Vendor-Specific Cisco (9,1) CiscoSecure-Defined-ACL	ACL name. ACS automatically sends this to the NAD as part of the RADIUS packet.
x			26	Vendor-Specific Cisco (9,1) sec:pg	Policy-based ACL assignment. Only applies to Catalyst 6000. sec:pg = <group-name>
	x	x	26	Vendor-Specific Cisco (9,1) url-redirect	Redirection URL. url-redirect = <URL>
	x	x	26	Vendor-Specific Cisco (9,1) url-redirect-acl	Apply the named ACL for the redirect URL; ACL must be defined locally on the NAD. Only works on switches with IOS. url-redirect-acl =< ACL-Name>
x	x	x	26	Vendor-Specific Cisco (9,1) posture-token	Posture token/state name. Automatically sent by ACS.
	x	x	26	Vendor-Specific Cisco (9,1) status-query-timeout	Sets Status Query timer
	x	x	26	Vendor-Specific Cisco (9,1) host-session-id	Session identifier used for auditing. Automatically sent by ACS.

Table 9-1 Attributes That Can Be Sent in the RADIUS-Accept Response (continued)

x	x	x	26	Vendor-Specific Microsoft = 311	Key for Status Query: MS-MPPE-Recv-Key Automatically sent by ACS.
x	x	x	27	Session-Timeout	Sets Revalidation Timer (in seconds)
x	x	x	29	Termination-Action	Action on Session Timeout (0) Default: Terminate session (1) Radius-Request: Re-authenticate
x			64	Tunnel-Type	13 = VLAN
x			65	Tunnel-Medium-Type	6 = 802
x	x	x	79	EAP Message	EAP Request/Response Packet in Access Request and Access Challenge: - EAP Success in Access Accept - EAP Failure in Access Reject
x	x	x	80	Message Authenticator	HMAC-MD5 to ensure integrity of packet.
x			81	Tunnel-Private-Group-ID	VLAN name

Step 6: Configure an External Posture Validation Audit Server

A NAC-enabled network might include agentless hosts that do not have the NAC client software. ACS can defer the posture validation of the agentless hosts to an audit server. The audit server determines the posture credentials of a host without relying on the presence of a PA.

Configuring an external audit server involves two stages:

- Adding the posture attribute to the ACS internal dictionary.
- Configuring an external posture validation server (audit server).

Add the Posture Attribute to the ACS Dictionary

Before you can create an external posture validation server, you must add one or more vendor attributes to the ACS internal data dictionary. To do this, you use the **bin\CSUtil** tool, which is located in the ACS installation directory.

To add the posture attributes:

Step 1 Create a text file in the *\Utils* directory with the following format:

```
[attr#0]
vendor-id=[your vendor id]
vendor-name=[The name of you company]
application-id=6
application-name=Audit
attribute-id=00003
attribute-name=Dummy-attr
attribute-profile=out
attribute-type=unsigned integer
```

Your vendor ID should be the Internet Assigned Numbers Authority (IANA)-assigned number that is the first section of the posture token attribute name, [vendor]:6:

Step 2 To install the attributes specified in the text file:

a. Open a DOS command window.

b. Enter the following command:

```
\<ACS_Install_Dir>\bin\CSUtil -addAVP [file_name]
```

where *ACS_Install_Dir* is the name of the ACS installation directory and *file_name* is the name of the text file that contains vendor attributes.

Step 3 Restart the **CSAdmin**, **CSLog**, and **CSAuth** services.

Configure the External Posture Validation Audit Server

You can configure an audit server once, and then use it for other profiles.

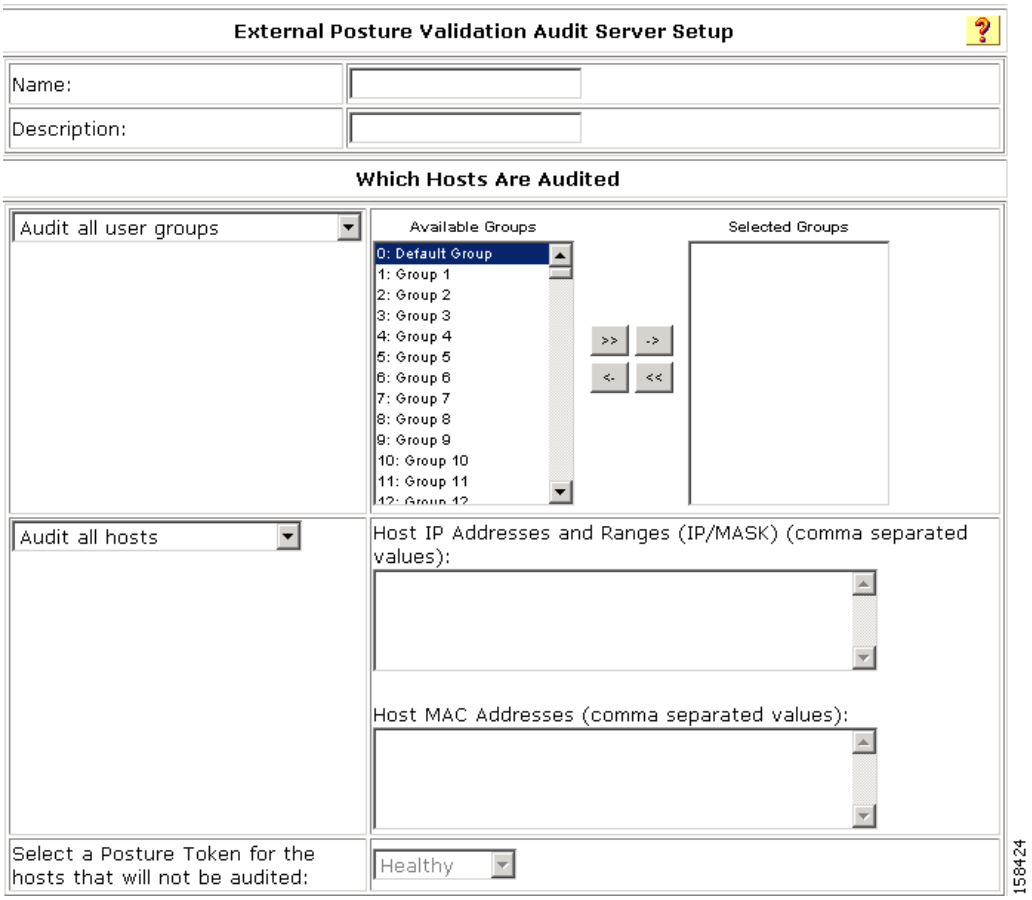
To configure an audit server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Audit Setup**.

Step 2 Click **Add Server**.

The External Posture Validation Audit Server Setup page appears, as shown in Figure 9-20.

Figure 9-20 External Posture Validation Audit Server Setup Page



Step 3 To configure the audit server:

a. Enter a Name and Description (optional).

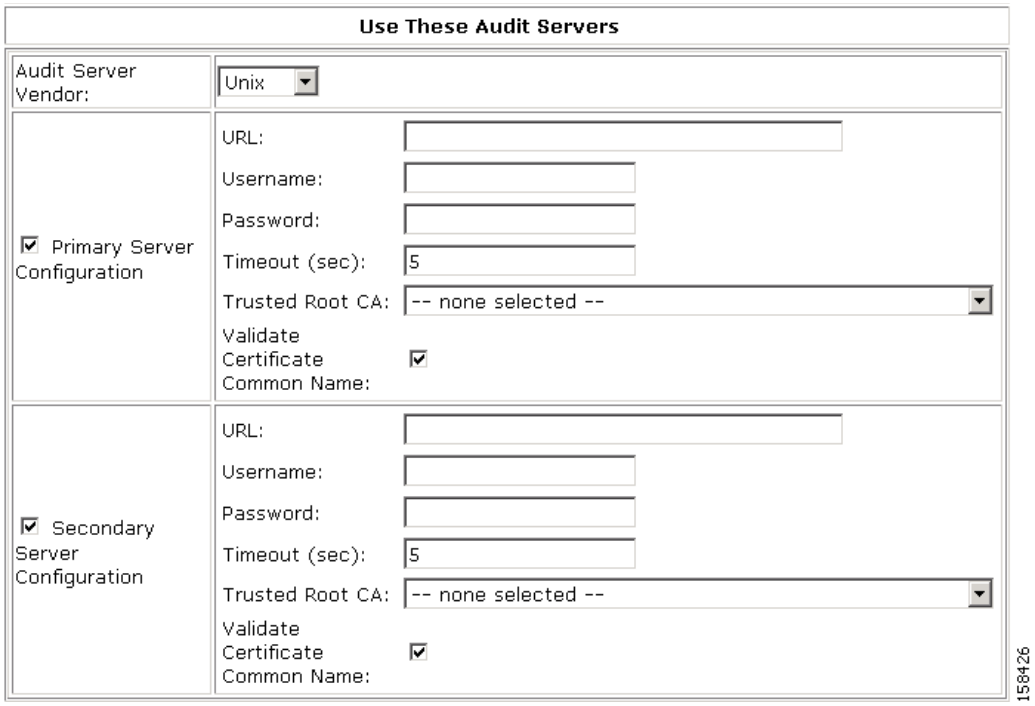
b. In the Which Hosts Are Audited section, choose what hosts you want to audit. You can enter the host IP or MAC addresses for the hosts that you want to audit or for a host that you do not want to audit.

c. For the hosts that will not be audited, choose a posture token from the drop-down list.

d. Scroll down to the Use These Audit Servers section.

Figure 9-21 shows the Use These Audit Servers section of the External Posture Validation Server Setup page.

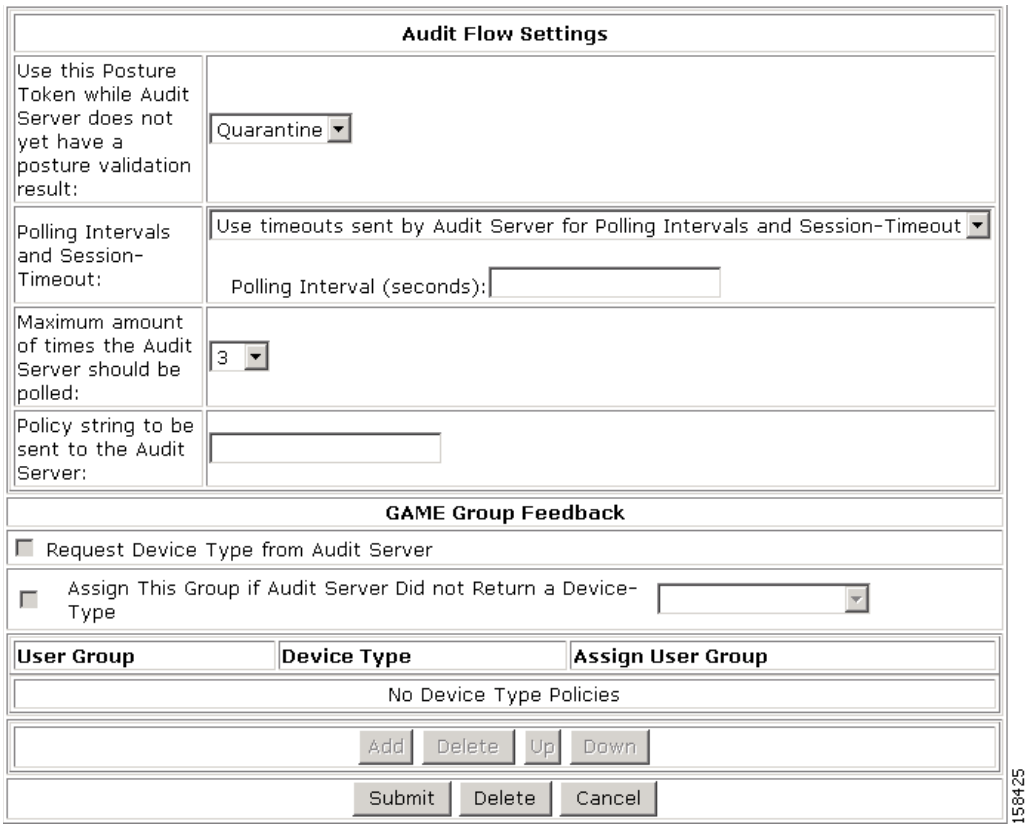
Figure 9-21 Use These Audit Servers Section



e. In the Use These Audit Servers section, enter the Audit Validation Server information, Audit Server vendor, URL, and password.

Figure 9-22 shows the Audit Flow Settings and the GAME Group Feedback section.

Figure 9-22 Audit Flow Settings and GAME Group Feedback Sections



f. If required, in the Audit Flow Setting section, set the audit-flow parameters.

g. If you are configuring GAME group feedback to support agentless host configuration in the NAC environment, configure the settings in the GAME Group Feedback section.

For information on configuring GAME Group Feedback settings, see Enable GAME Group Feedback, page 9-79.

h. Click **Submit**.

Step 7: Configure Posture Validation for NAC

This section describes how to set up simple posture validation for a NAC-enabled network. You can create internal policies that ACS uses to validate the posture data or you can configure ACS to send the posture data to an external posture validation server.

Configure Internal Posture Validation Policies

An *internal posture validation policy* is an internal attribute policy that you can use in more then one profile. The result of an internal posture validation policy returns a Posture Assessment (*token*) according to rules that you set.

To create an internal posture validation policy:

Step 1 In the navigation bar, click **Posture Validation**.

The Posture Validation Components Setup page opens.

Step 2 Click **Internal Posture Validation Setup**.

The Posture Validation page opens, which lists any existing posture validation policies.

Step 3 Choose **Add Policy**.

The Edit Posture Validation page opens.

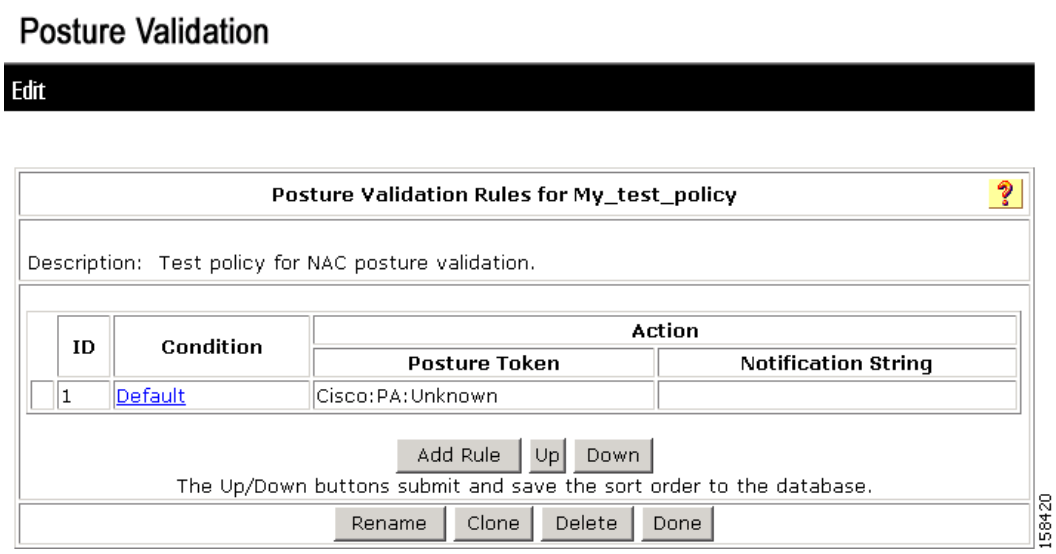
Step 4 Enter a name for the policy.

Step 5 Enter a Description (optional).

Step 6 Click **Submit**.

A new internal policy is created with a default rule. Figure 9-23 shows an example policy.

Figure 9-23 Creating a New Posture Validation Policy



Step 7 To edit the default rule:

a. Click on the **Default** link.

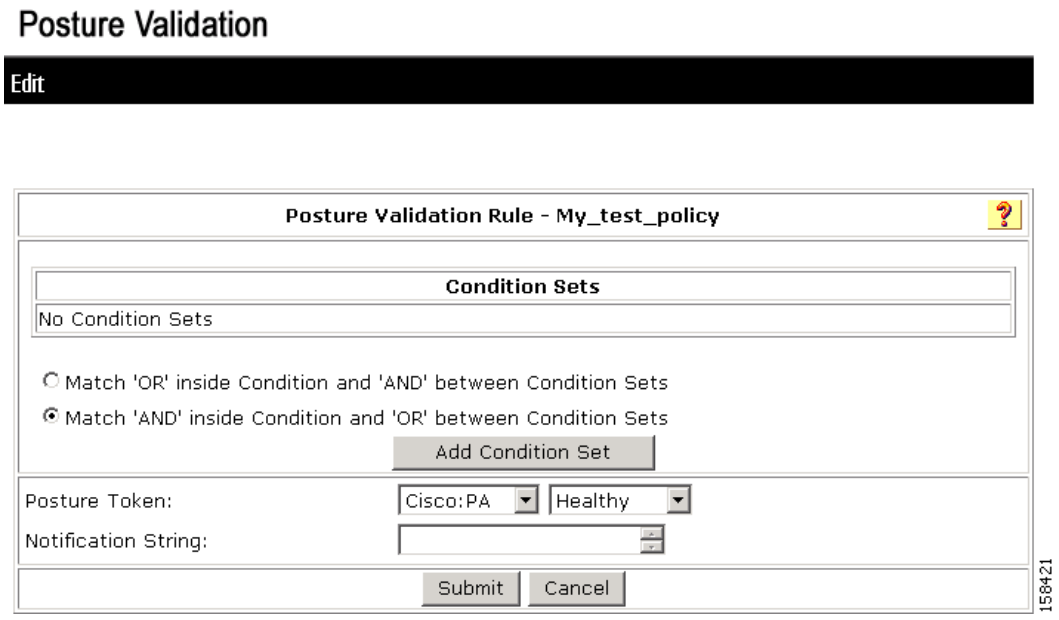
b. Choose a new Posture Assessment and Notification String for the default rule.

Step 8 To add a new rule:

a. Click **Add Rule**.

The Edit Posture Rule page appears, as shown in Figure 9-24. Initially no conditions are available for the rule.

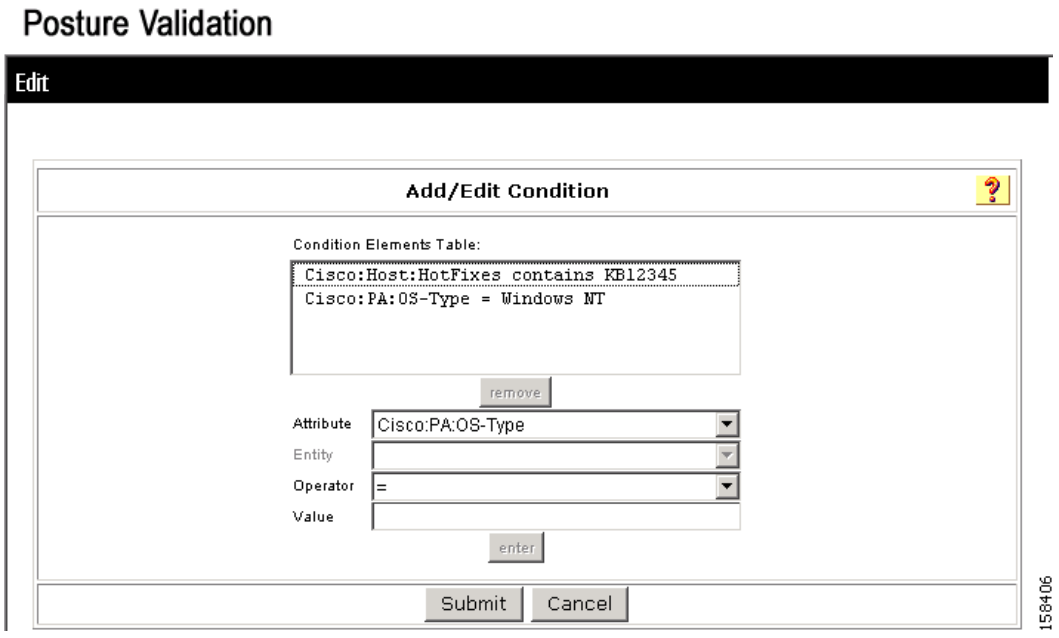
Figure 9-24 Edit Posture Validation Rule Page



b. Click **Add Condition Set**.

c. The Add/Edit Condition page appears, as shown in Figure 9-25.

Figure 9-25 Add/Edit Condition Page



d. From the **Attribute** drop-down list, choose an Attribute value.

e. From the Operator drop-down list, choose a condition.

f. In the Value text box, enter a value for the condition.

g. Click **Enter**.

The specified rule appears in Add/Edit Condition page, as shown in Figure 9-25.

h. Enter additional conditions as required.

i. Click **Submit**.

j. Click **Apply and Restart** to apply the new posture validation rule(s).

Configure External Posture Validation Policies

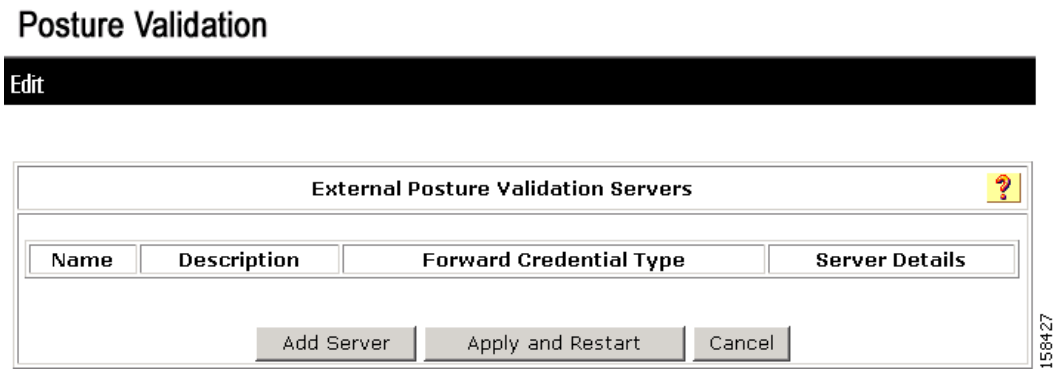
An external posture validation policy uses an external server that returns a posture assessment (token) to ACS according to data that the ACS forwards to this server.

To set up an external posture validation server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Setup**.

Step 2 The Edit External Posture Validation Servers page opens, as shown in Figure 9-26.

Figure 9-26 Edit External Posture Validation Servers Page

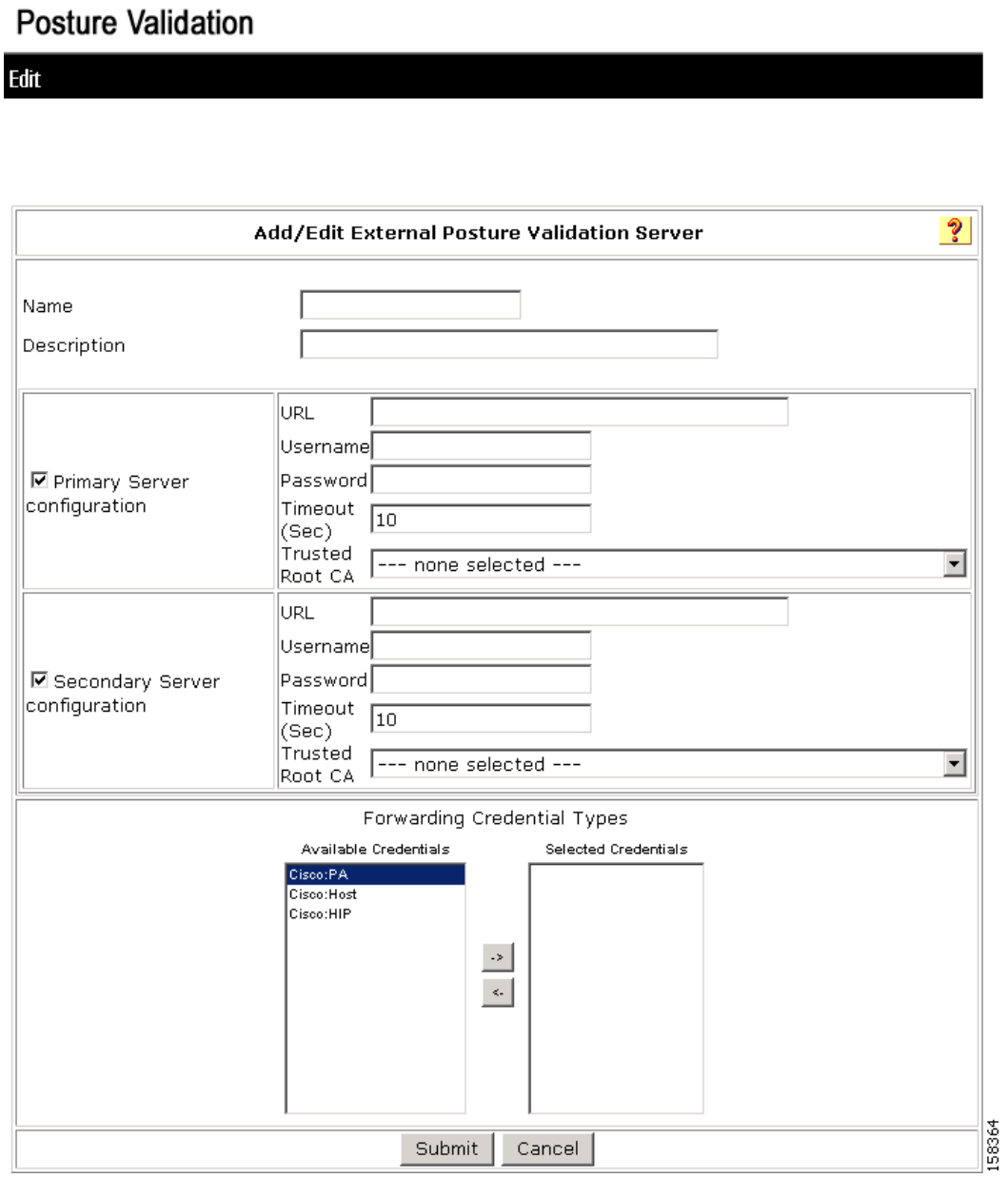


Initially, the list of external posture validation servers is empty.

Step 3 Click **Add Server**.

The Add/Edit External Posture Validation Server page appears, as shown in Figure 9-27.

Figure 9-27 Add/Edit External Posture Validation Server Page



Step 4 Enter a Name and Description (optional).

Step 5 Enter the server details, URL, User, Password, Timeout, and certificate (if required by the antivirus server).

Step 6 Click **Submit**.

Configure an External Posture Validation Audit Server

A NAC-enabled network might include agentless hosts that do not have the NAC client software. ACS can defer the posture validation of the agentless hosts to an audit server. The audit server determines the posture credentials of a host without relying on the presence of a PA.

Configuring an external audit server involves two stages:

- Adding the posture attribute to the ACS internal dictionary.
- Configuring an external posture validation server (audit server).

Add the Posture Attribute to the ACS Dictionary

Before you can create an external posture validation server, you must add one or more vendor attributes to the ACS internal data dictionary. To do this, you use the **bin\CSUtil** tool, which is located in the ACS installation directory.

To add the posture attributes:

Step 1 Create a text file in the *Utils* directory with the following format:

```
[attr#0]
vendor-id=[your vendor id]
vendor-name=[The name of you company]
application-id=6
application-name=Audit
attribute-id=00003
attribute-name=Dummy-attr
attribute-profile=out
attribute-type=unsigned integer
```

Your vendor ID should be the Internet Assigned Numbers Authority (IANA)-assigned number that is the first section of the posture token attribute name, [vendor]:6:

Step 2 To install the attributes specified in the text file:

a. Open a DOS command window.

b. Enter the following command:

\<*ACS_Install_Dir*>\bin\CSUtil –addAVP [*file_name*]

where *ACS_Install_Dir* is the name of the ACS installation directory and *file_name* is the name of the text file that contains vendor attributes.

Step 3 Restart the **CSAdmin**, **CSLog**, and **CSAuth** services.

Configure the External Posture Validation Audit Server

You can configure an audit server once, and then use it for other profiles.

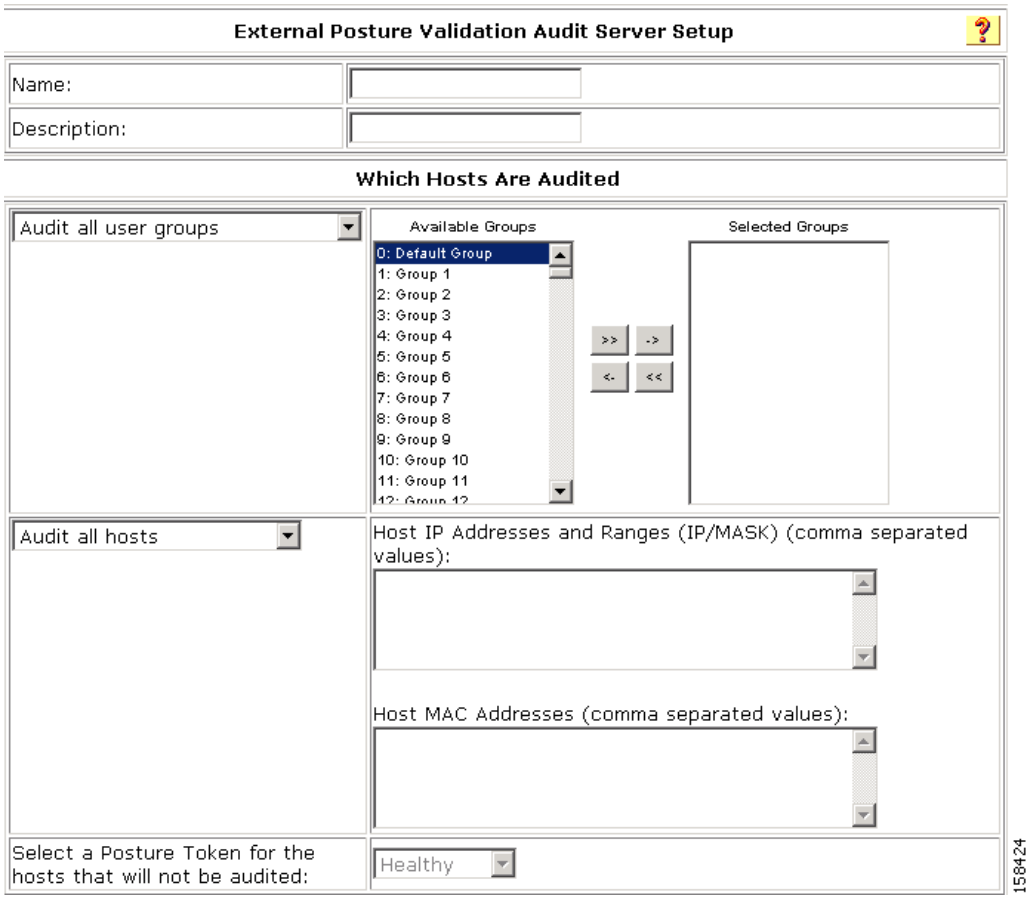
To configure an audit server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Audit Setup**.

Step 2 Click **Add Server**.

The External Posture Validation Audit Server Setup page appears, as shown in Figure 9-28.

Figure 9-28 External Posture Validation Audit Server Setup Page



Step 3 To configure the audit server:

a. Enter a Name and Description (optional).

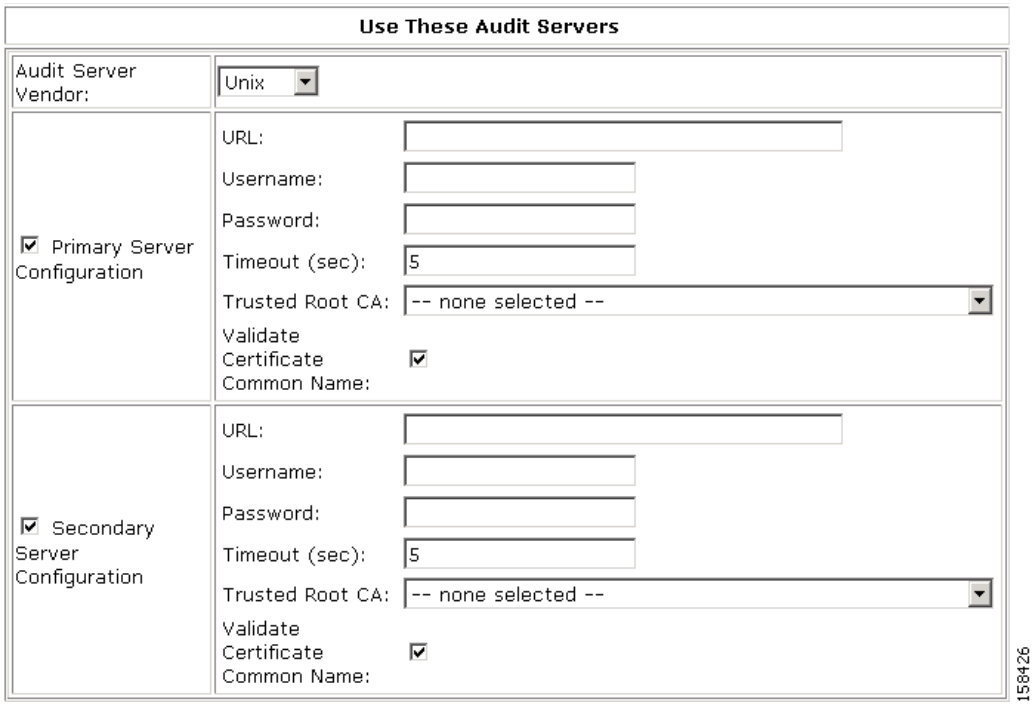
b. In the Which Hosts Are Audited section, choose what hosts you want to audit. You can enter the host IP or MAC addresses for the hosts that you want to audit or for a host that you do not want to audit.

c. For the hosts that will not be audited, choose a posture token from the drop-down list.

d. Scroll down to the Use These Audit Servers section.

Figure 9-29 shows the Use These Audit Servers section of the External Posture Validation Server Setup page.

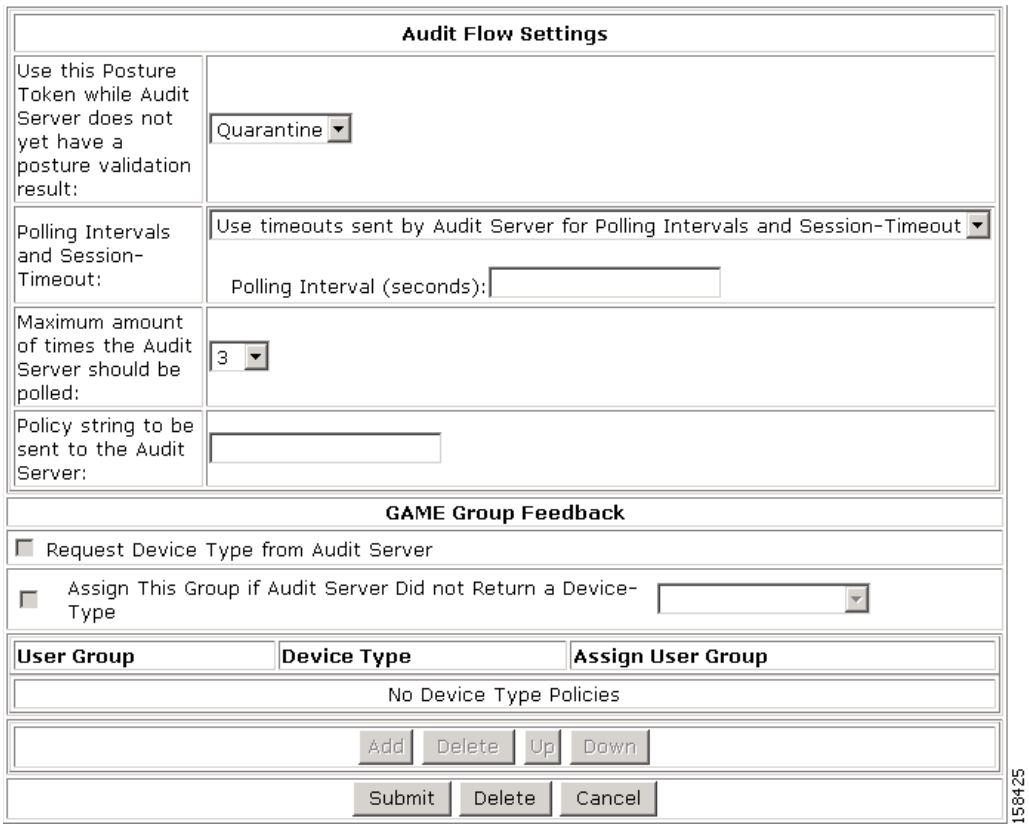
Figure 9-29 Use These Audit Servers Section



e. In the Use These Audit Servers section, enter the Audit Validation Server information, Audit Server vendor, URL, and password.

Figure 9-30 shows the Audit Flow Settings and the GAME Group Feedback section.

Figure 9-30 Audit Flow Settings and GAME Group Feedback Sections



f. If required, in the Audit Flow Setting section, set the audit-flow parameters.

g. If you are configuring GAME group feedback to support agentless host configuration in the NAC environment, configure the settings in the GAME Group Feedback section.

For information on configuring GAME Group Feedback settings, see Enable GAME Group Feedback, page 9-79.

h. Click **Submit**.

Authorization Policy and NAC Audit

Audit servers define two types of posture assessments (tokens). A:

- Temporary posture assessment is used as the *in progress* assessment. ACS grants the in progress posture assessment to the agentless host while the audit server is processing the auditing on the host and does not have a final result.
- *Final* posture assessment is the posture assessment that the audit server returns after it completes the auditing process.

To configure the authorization policy to work with the audit server, at least two RACs or downloadable ACLs are required: one for the in progress posture assessment and one for the final posture assessment. You should use a separate RAC or downloadable ACL for each token.

Step 8: Set Up Templates to Create NAPs

ACS 4.1 provides several profile templates that you can use to configure common usable profiles. In NAC-enabled networks, you can use these predefined profile templates to configure commonly used profiles. This section describes the templates provided in ACS 4.1.

Sample NAC Profile Templates

ACS 4.1 provides the following sample profile templates for NAC. A:

- NAC Layer 3 profile template (NAC L3 IP)
- NAC Layer 2 profile template (NAC L2 IP)
- NAC Layer 2 802.1x template (NAC L2 802.1x)
- Wireless (NAC L2 802.1x) template

In addition to these templates, ACS 4.1 provides two templates for agentless host processing that you can use in NAC installations:

- Agentless Host for Layer 3 profile template
- Agentless Host for Layer 2 (802.1x) profile template

Sample NAC Layer 3 Profile Template

This template creates a profile for Layer 3 NAC requests. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a Layer 3 NAC profile template:

Step 1 Check the check boxes for the following options in the Global Authentication Setup page:

- Allow Posture Validation
- EAP-FAST
- EAP-FAST MS-CHAPv2
- EAP-FAST GTC

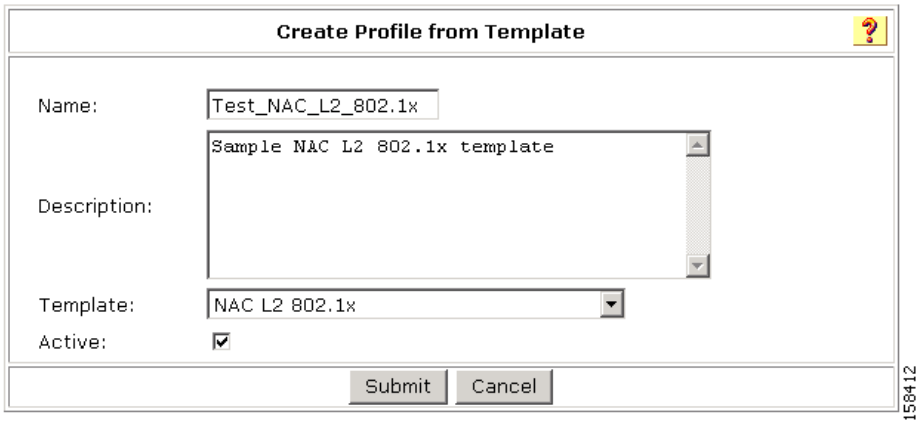
Step 2 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 3 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 9-31.

Figure 9-31 Create Profile From Template Page



Step 4 Enter a Name and Description (optional).

Step 5 From the **Template** drop-down list, choose **NAC L3 IP**.

Step 6 Check the **Active** check box.

Step 7 Click **Submit**.

If no error appears, then you have created a profile that can authenticate Layer 3 NAC hosts.

The Edit Network Access Profile page opens, and the new profile appears in the Name column.

The predefined values for the Layer 3 NAC template include:

- Profile Setup options
- Protocols
- A sample posture validation policy
- Authentication policy

Step 8 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

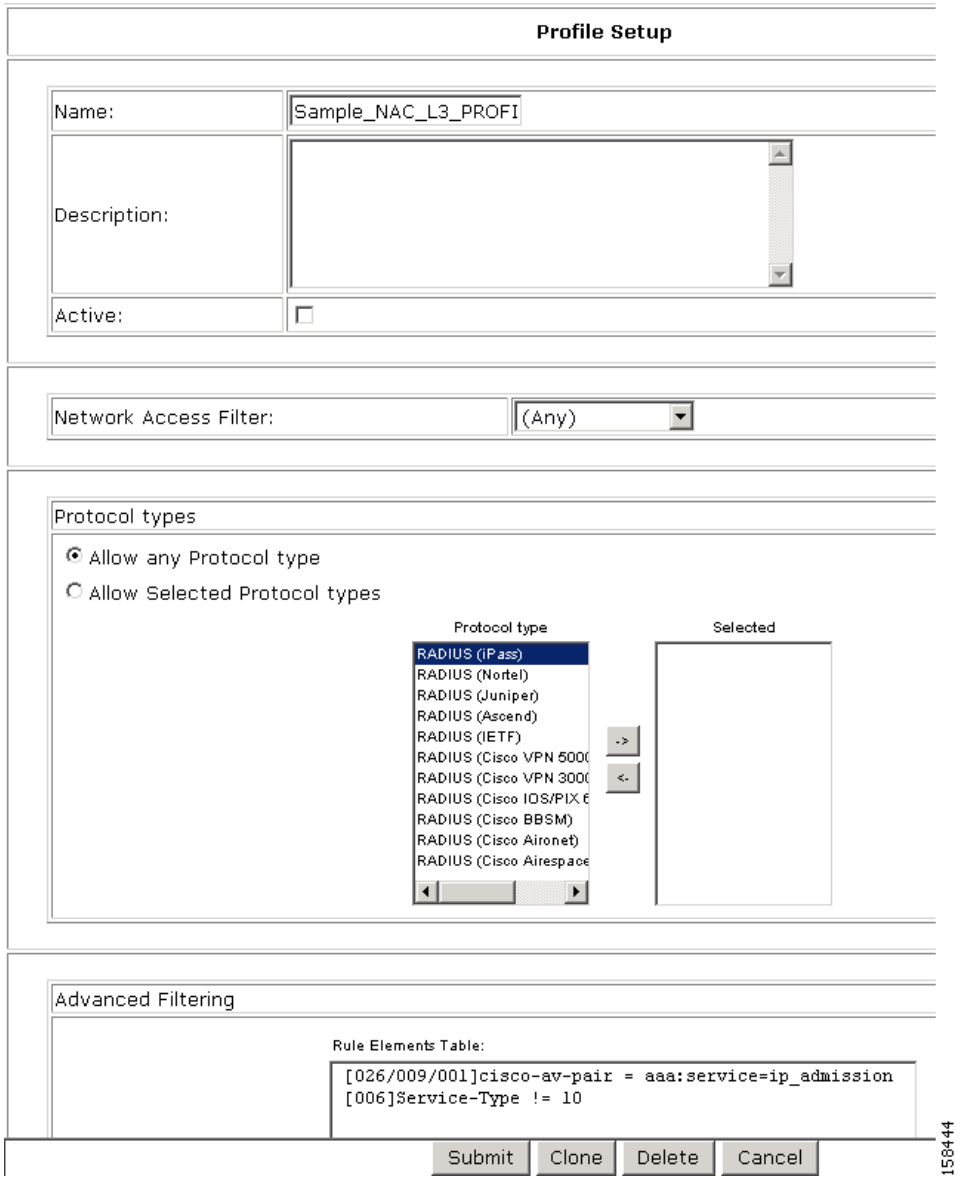
To use the Profile Setup settings from the template:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 9-32.

Figure 9-32 Profile Setup Page for Layer 3 NAC Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

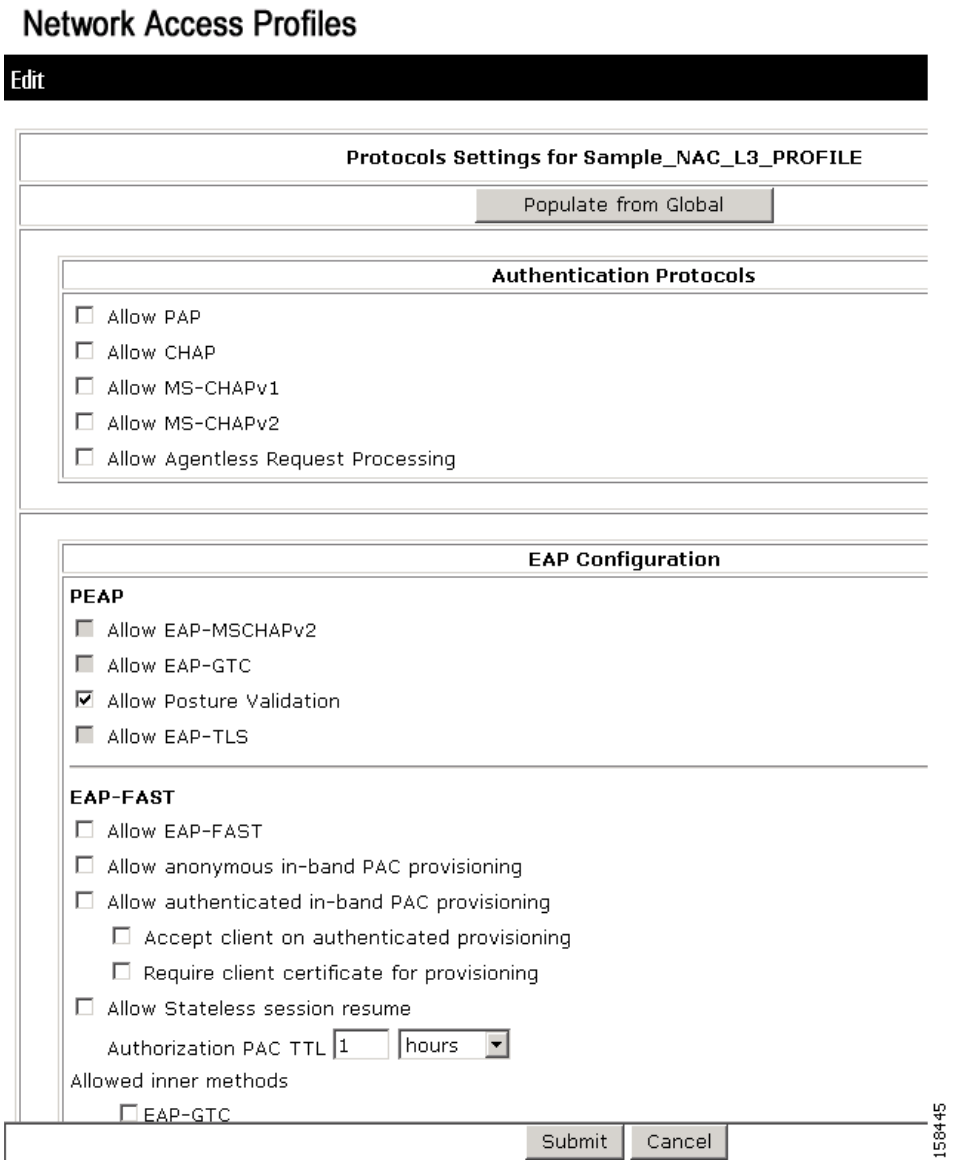
```
[026/009/001]Cisco-av-pair = aaa:service=ip admission
[006]Service-Type != 10
```

These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy for the NAC Layer 3 Template

Figure 9-33 shows the Protocols settings for the NAC Layer 3 template.

Figure 9-33 Protocols Setting for NAC Layer 3 Template



In the EAP Configuration section, Posture Validation is enabled.

Authentication Policy

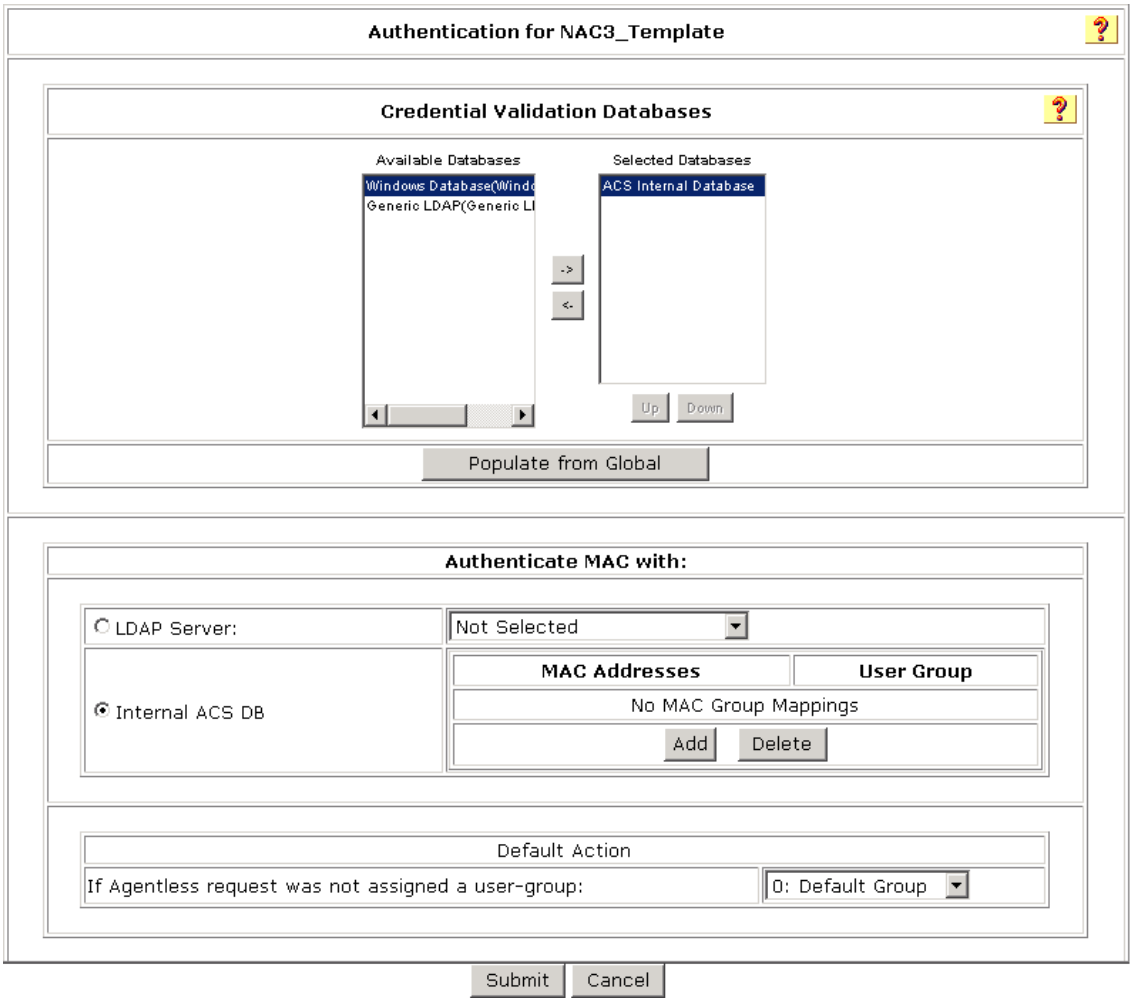
To configure authentication policy:

Step 1 In the navigation bar, select **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication page for the profile opens, as shown in Figure 9-34.

Figure 9-34 Authentication Page for Layer 3 NAC Profile Template



On this page, you can see the Layer 3 NAC template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

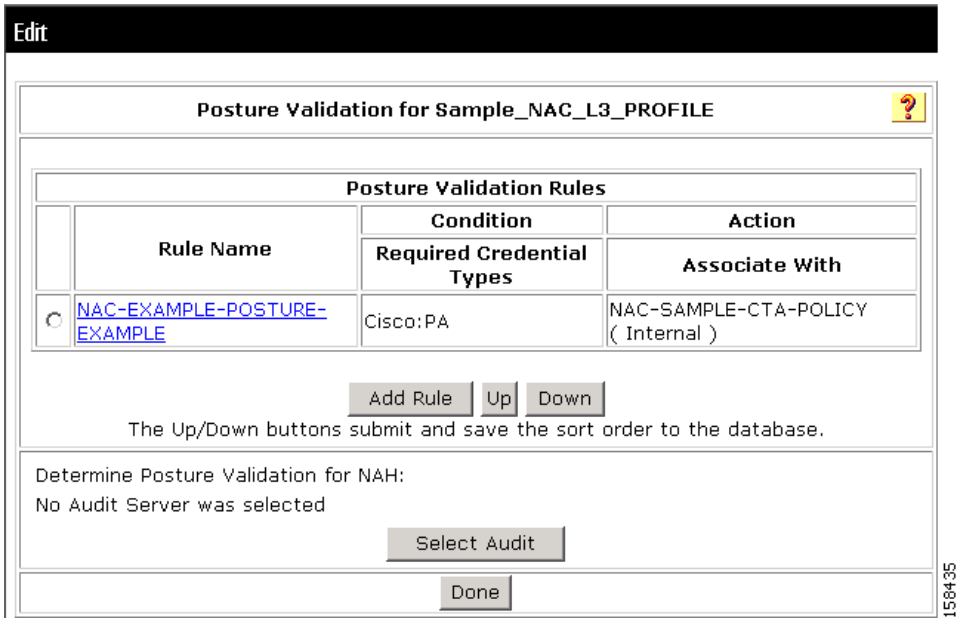
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 9-35 shows the sample posture validation policy provided with the NAC Layer 3 template.

Figure 9-35 Sample Posture Validation Policy for NAC Layer 3 Template



Sample NAC Layer 2 Template

This template creates a profile for Layer 2 NAC requests.

Before you use the Layer 2 NAC profile template:

1. Select **EAP-FAST Configuration** in **Global Authentication Settings**.
2. Check (enable) the **Allow authenticated in-band PAC provisioning**.
3. Check (enable) **EAP-GTC** and **EAP-MSCHAPv2**.

To create a Layer 2 NAC profile template:

Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **NAC L2 IP**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate Layer 2 NAC hosts and the Profile Setup page for the NAC Layer 2 template appears.

The predefined values for the Layer 2 NAC template include:

- Profile Setup
- Protocols settings
- Authentication policy
- A sample posture validation rule

  The name of this policy is NAC-EXAMPLE-POSTURE-EXAMPLE.

Step 7 To select a configuration option, click the option name.

Profile Setup

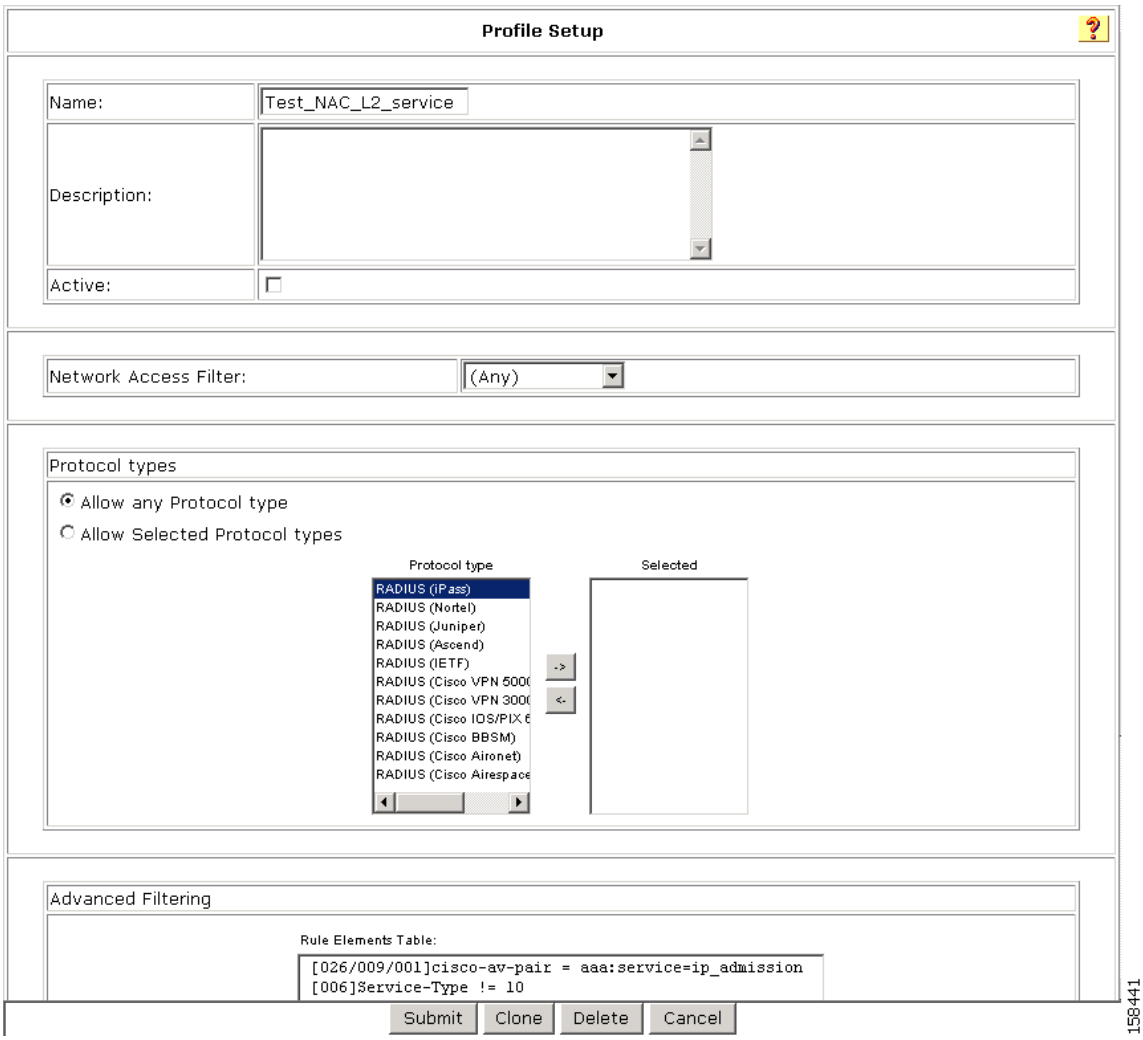
To enable the profile setup:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the Profile that you created.

The Profile Setup page appears, as shown in Figure 9-36.

Figure 9-36 Profile Setup Page for NAC Layer 2 Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can select the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

  ```
  [026/009/001]Cisco-av-pair = aaa:service=ip admission
  [006]Service-Type != 10
  ```

  These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

This template automatically sets Advanced Filtering and Authentication properties with NAC Layer 2 IP Configuration.

ACS and Attribute-Value Pairs

When you enable NAC Layer 2 IP validation, ACS provides NAC AAA services by using RADIUS. ACS gets information about the antivirus credentials of the endpoint system and validates the antivirus condition of the endpoint.

You can set these Attribute-Value (AV) pairs on ACS by using the RADIUS cisco-av-pair vendor-specific attributes (VSAs).

- **Cisco Secure-Defined-ACL**—Specifies the names of the downloadable ACLs on the ACS. The switch gets the ACL name from the Cisco Secure-Defined-ACL AV pair in this format:

  #ACL#-IP-name-number

  where *name* is the ACL name and *number* is the version number, such as 3f783768.

  ACS uses the Auth-Proxy posture code to check if the switch has downloaded access-control entries (ACEs) for the specified downloadable ACL. If the switch has not downloaded the ACES, ACS sends an AAA request with the downloadable ACL name as the username so that the switch downloads the ACEs. The downloadable ACL is then created as a named ACL on the switch. This ACL has ACEs with a source address of **Any** and does not have an implicit **Deny** statement at the end. When the downloadable ACL is applied to an interface after posture validation is complete, the source address is changed from any to the host source IP address. The ACEs are prepended to the downloadable ACL that is applied to the switch interface to which the endpoint device is connected.

  If traffic matches the Cisco Secure-Defined-ACL ACEs, ACS takes appropriate actions required by NAC.

- **url redirect and url-redirect-acl**—Specifies the local URL policy on the switch. The switches use these cisco-av-pair VSAs:

  — *url-redirect = <HTTP or HTTPS URL>*

  — *url-redirect-acl = switch ACL name*

  These AV pairs enable the switch to intercept an HTTP or Secure HTTP (HTTPS) request from the endpoint device and forward the client web browser to the specified redirect address from which the latest antivirus files can be downloaded. The `url-redirect` AV pair on the ACS contains the URL to which the web browser will be redirected. The `url-redirect-acl` AV pair contains the name of an ACL which specifies the HTTP or HTTPS traffic to be redirected. The ACL must be defined on the switch. Traffic which matches a permit entry in the redirect ACL will be redirected.

  If the host's posture is not healthy, ACS might send these AV pairs.

For more information about AV pairs that Cisco IOS software supports, see the documentation about the software releases that run on the AAA clients.

Default ACLs

If you configure NAC Layer 2 IP validation on a switch port, you must also configure a default port ACL on a switch port. You should also apply the default ACL to IP traffic for hosts that have not completed posture validation.

If you configure the default ACL on the switch and the ACS sends a host access policy to the switch, the switch applies the policy to traffic from the host that is connected to a switch port. If the policy applies to the traffic, the switch forwards the traffic. If the policy does not apply, the switch applies the default ACL. However, if the switch gets a host access policy from the ACS, but the default ACL is not configured, the NAC Layer 2 IP configuration does not take effect.

When ACS sends the switch a downloadable ACL that specifies a redirect URL as a policy-map action, this ACL takes precedence over the default ACL that is already configured on the switch port. The default ACL also takes precedence over the policy that is already configured on the host. If the default port ACL is not configured on the switch, the switch can still apply the downloadable ACL from ACS.

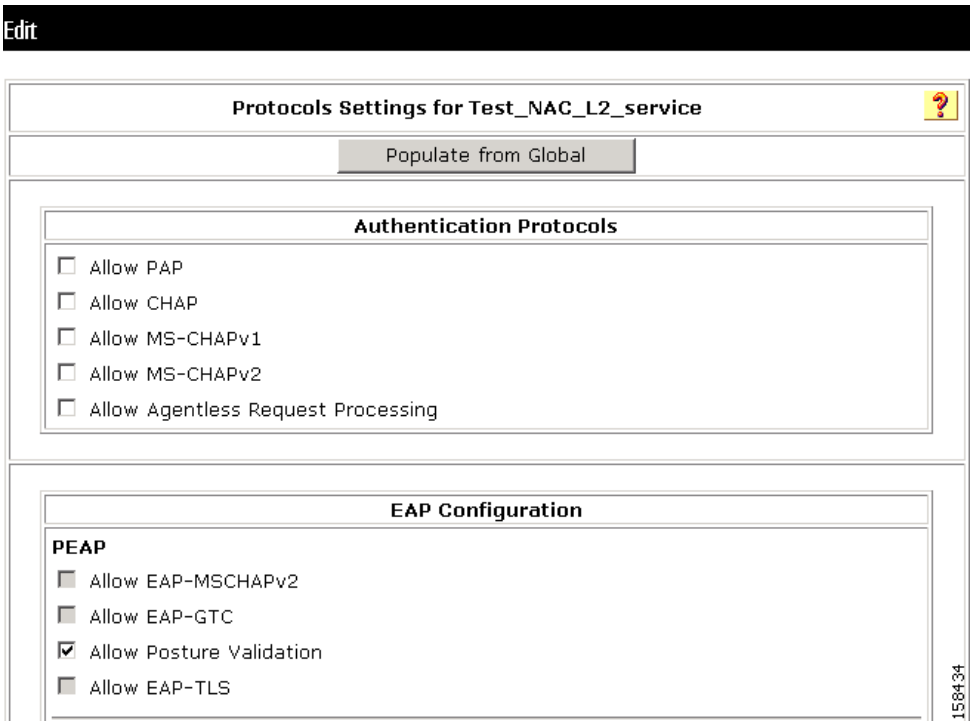
You use this template for access requests from Layer 2 devices that do not have the 802.1x client installed. The Authentication Bypass (802.1x fallback) template is used for access requests to bypass the nonclient authentication process. Users are mapped to a User Group based on their identity.

Note Do not click the **Populate from Global** button; otherwise, the settings for this authentication field will be inherited from the settings in the Global Authentication Setup in System Configuration.

Protocols Settings

Figure 9-37 shows the Protocols settings for the NAC Layer 2 template.

Figure 9-37 Protocols Setting for NAC Layer 2 Template



On this page, you can see the Layer 2 NAC template configuration for protocols. The default settings are:

- In the EAP Configuration area, posture validation is enabled.
- **Allow EAP-Fast Configuration** is checked, which means that this profile allows EAP-FAST authentication.

Authentication Policy

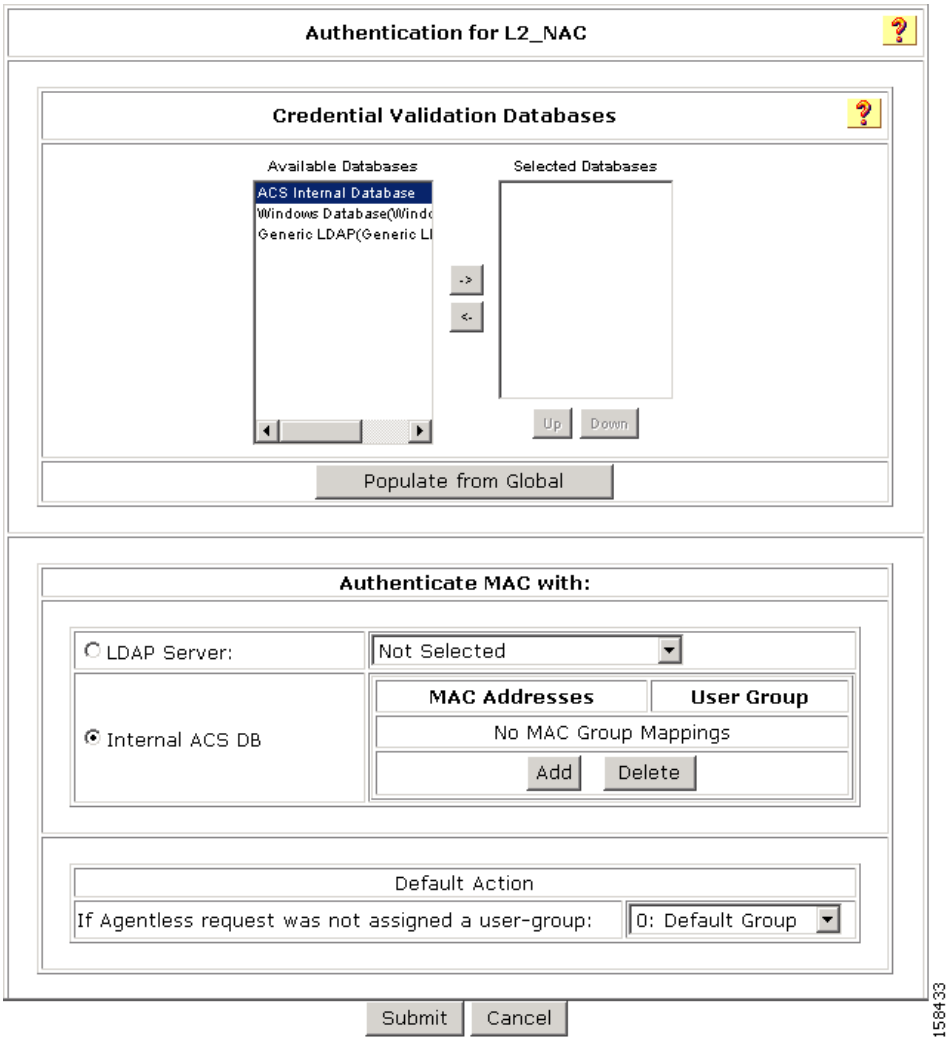
To set the authentication policy:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication Settings page for the NAC Layer 2 template opens, as shown in Figure 9-38.

Figure 9-38 Authentication Settings for NAC Layer 2 Template



Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

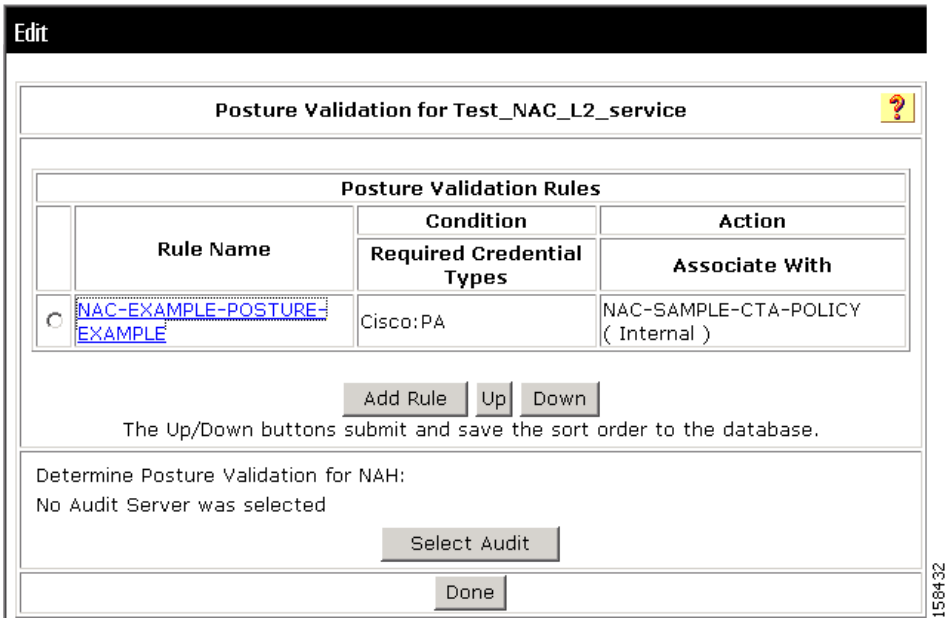
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 9-39 shows the sample posture validation rule provided with the NAC Layer 2 template.

Figure 9-39 Sample Posture Validation Policy for NAC Layer 2 Template



Sample NAC Layer 2 802.1x Template

This template creates a profile for Layer 2 NAC 802.1x requests. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a Layer 2 NAC 802.1x profile template:

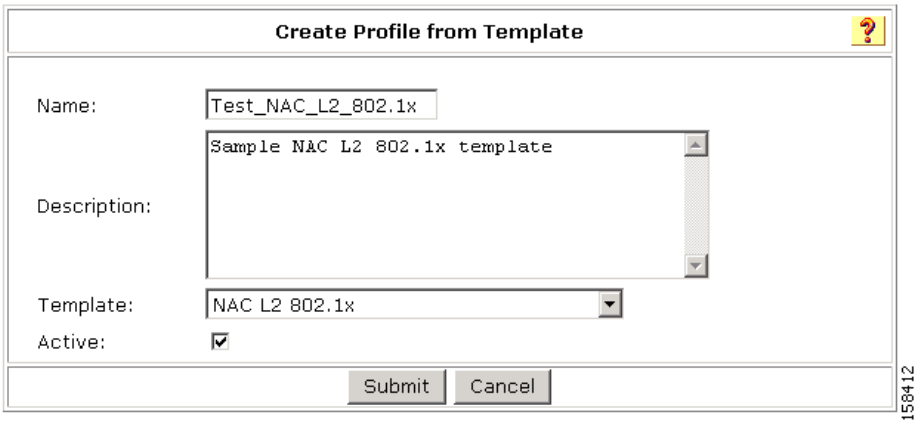
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 9-40.

Figure 9-40 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **NAC L2 802.1x**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate Layer 2 NAC hosts.

The Edit Network Access Profile page opens, and the new profile appears in the Name column.

The predefined values for the Layer 2 NAC 802.1x template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

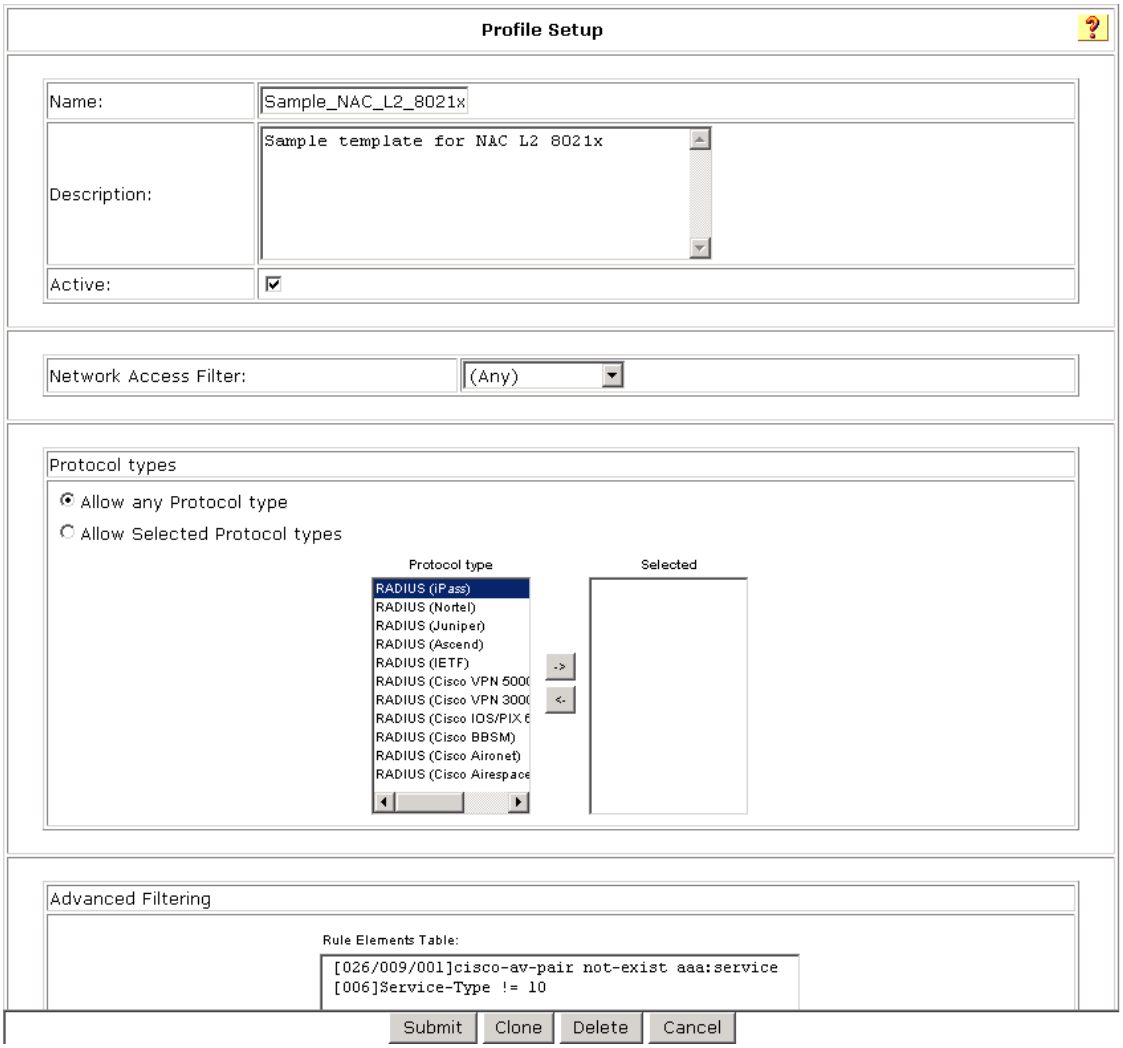
To use the Profile Setup settings from the template:

Step 1 In the navigation bar, click **Network Access Profiles**.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 9-41.

Figure 9-41 Profile Setup Page for NAC Layer 2 802.1x Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can select the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

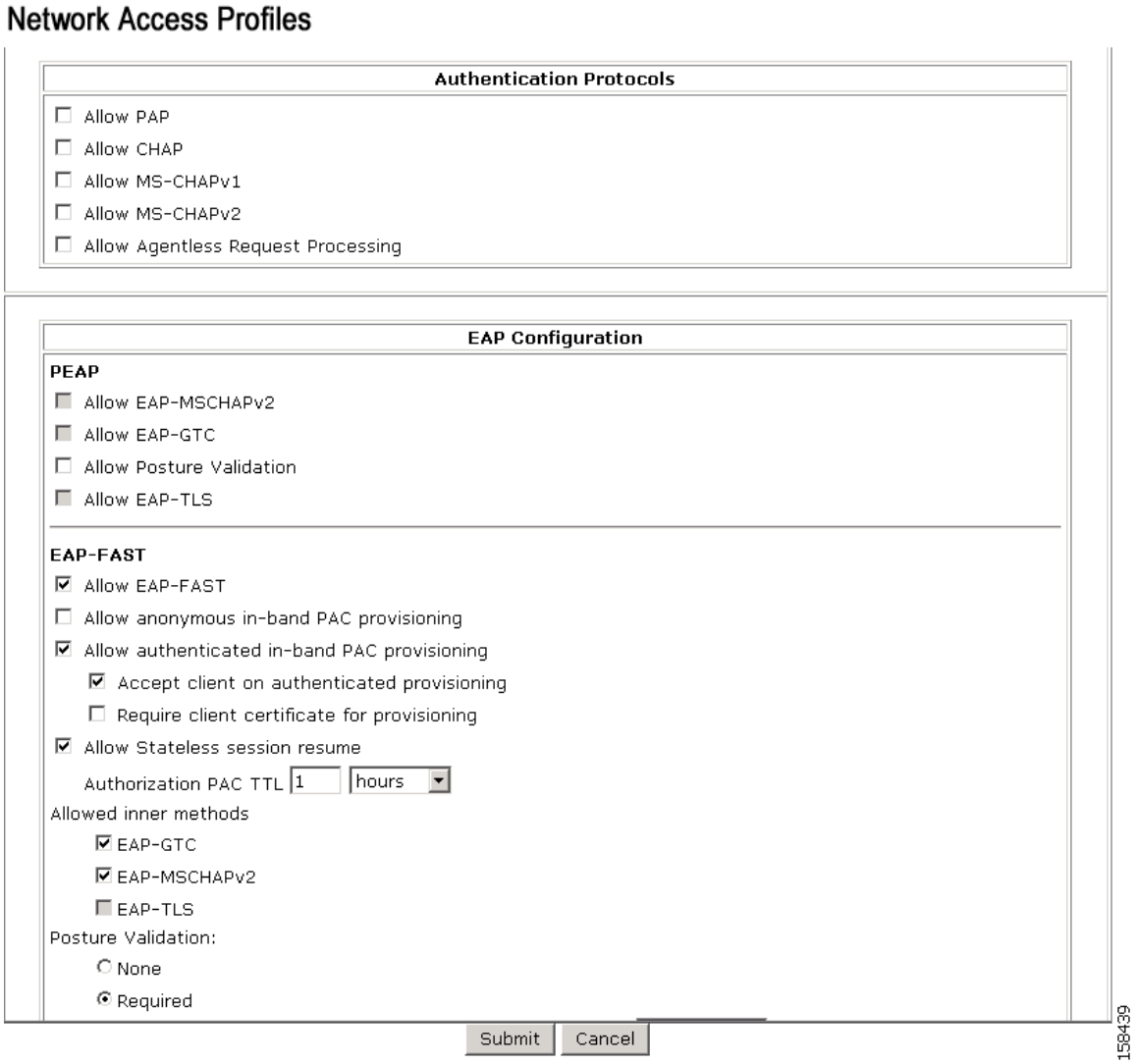
  ```
  [026/009/001]Cisco-av-pair = aaa:service=ip admission
  [006]Service-Type != 10
  ```

  These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 9-42 shows the Protocols settings for the NAC Layer 2 802.1x template.

Figure 9-42 Protocols Setting for NAC Layer 802.1x Template



In the EAP Configuration section, Posture Validation is enabled.

Authorization Policy

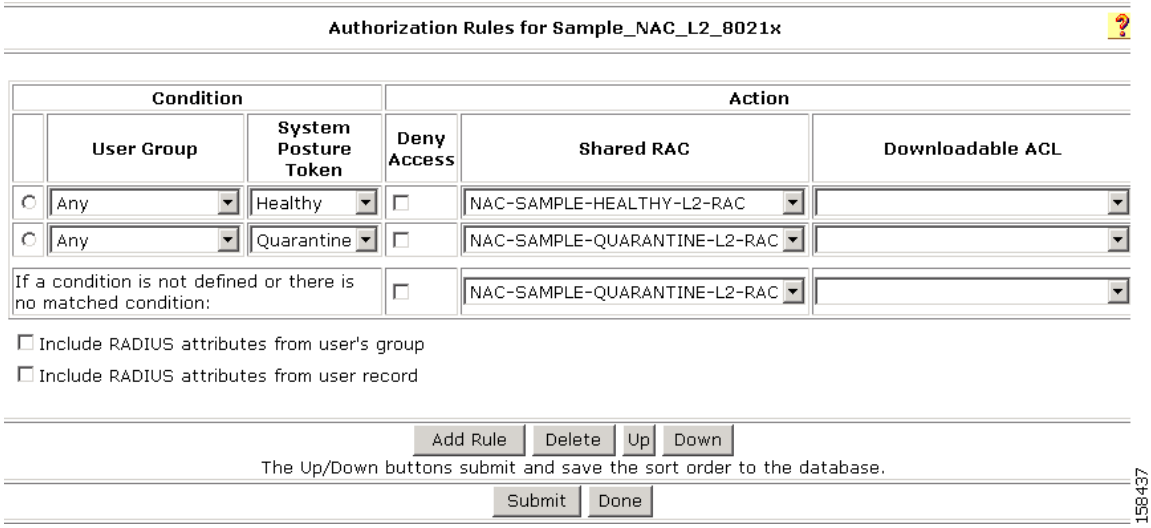
To configure an authorization policy for the NAC Layer 2 802.1x template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authorization** link from the Policies column.

The Authentication page for the NAC Layer 2 802.1x template profile appears, as shown in Figure 9-43.

Figure 9-43 Authentication Page for NAC Layer 2 802.1x Profile Template



On this page, you can see the Layer 2 NAC 802.1x template configuration for authorization.

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

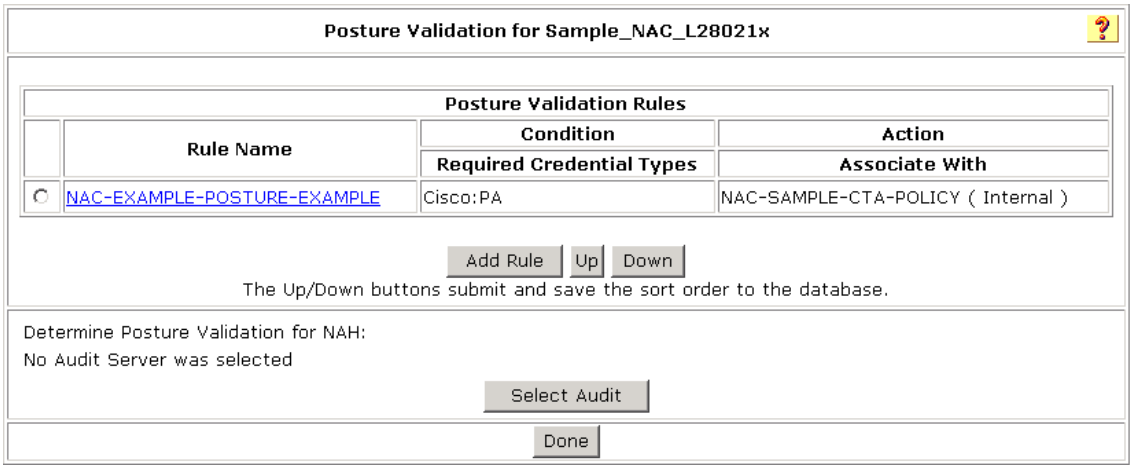
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 9-44 shows the sample posture validation policy provided with the NAC Layer 2 802.1x template.

Figure 9-44 Sample Posture Validation Policy for NAC Layer 2 802.1x Template



Sample Wireless (NAC L2 802.1x) Template

This template creates a profile for Layer 2 NAC 802.1x requests in wireless networks. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create a wireless (NAC L2 802.1x) NAC profile template:

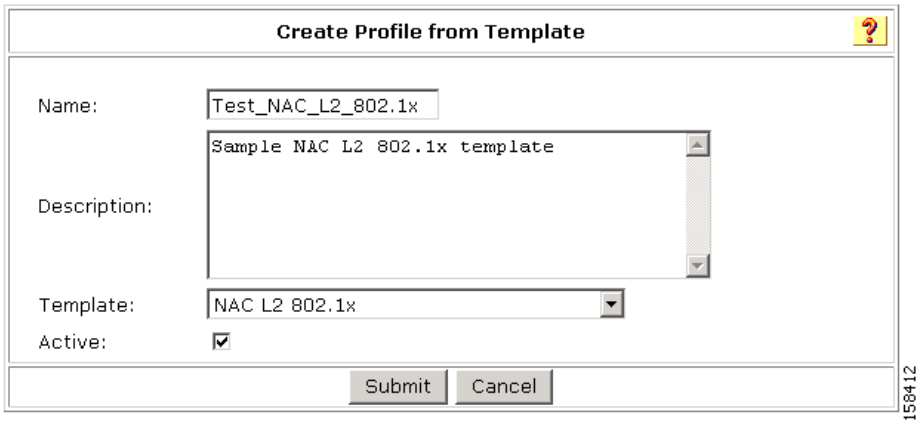
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 9-45.

Figure 9-45 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the Template drop-down list, choose **Wireless (NAC L2 802.1x)**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a Profile that can authenticate wireless NAC Layer 2 802.1x hosts.

The Edit Network Access Profile page opens, and the new profile is listed in the Name column.

The predefined values for the NAC Layer 2 802.1x template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options:

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

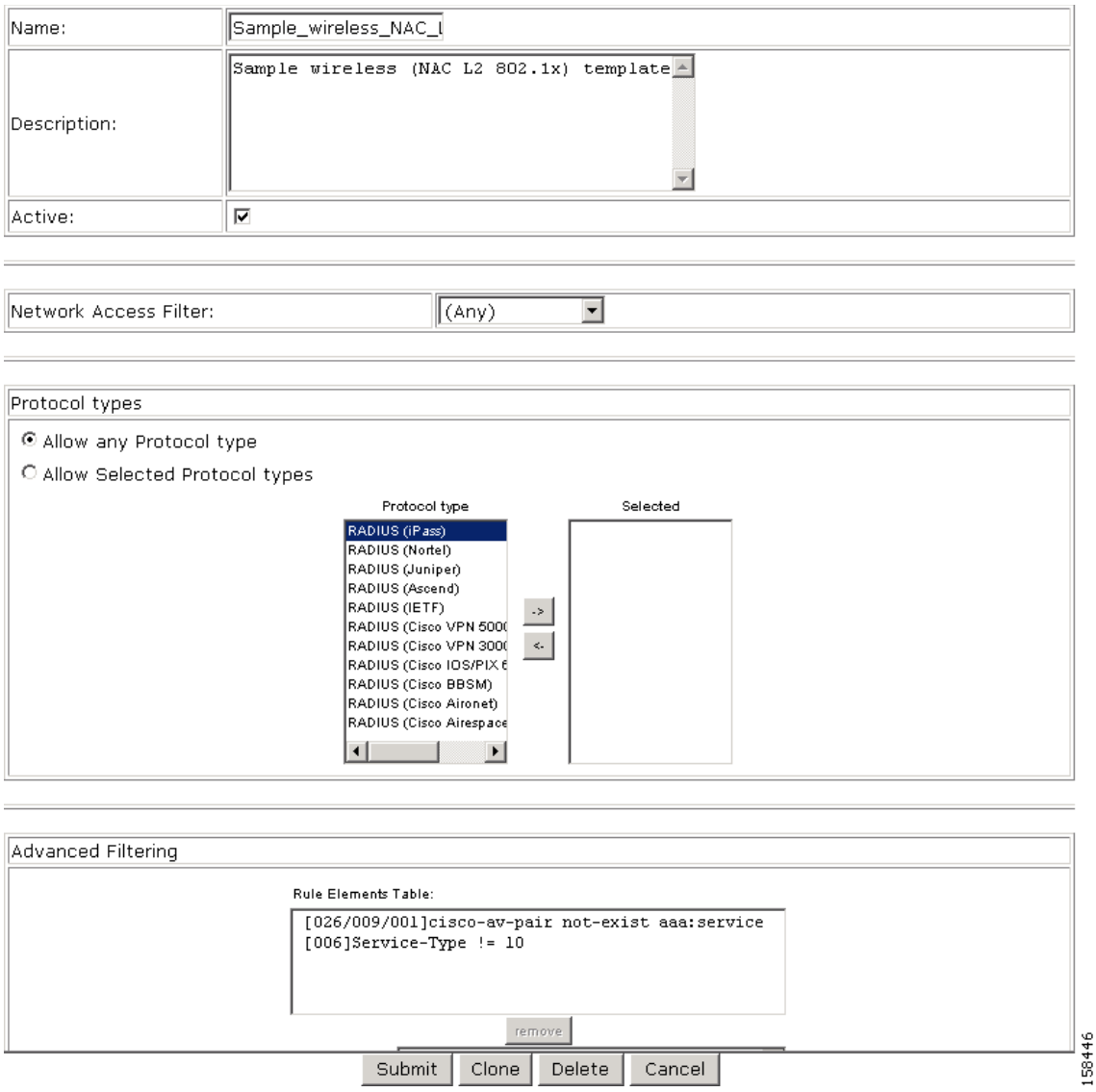
To use the Profile Setup settings from the template:

Step 1 Go to Network Access Profiles.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 9-46.

Figure 9-46 Profile Setup Page for Wireless (NAC L2 802.1x)Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.
- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

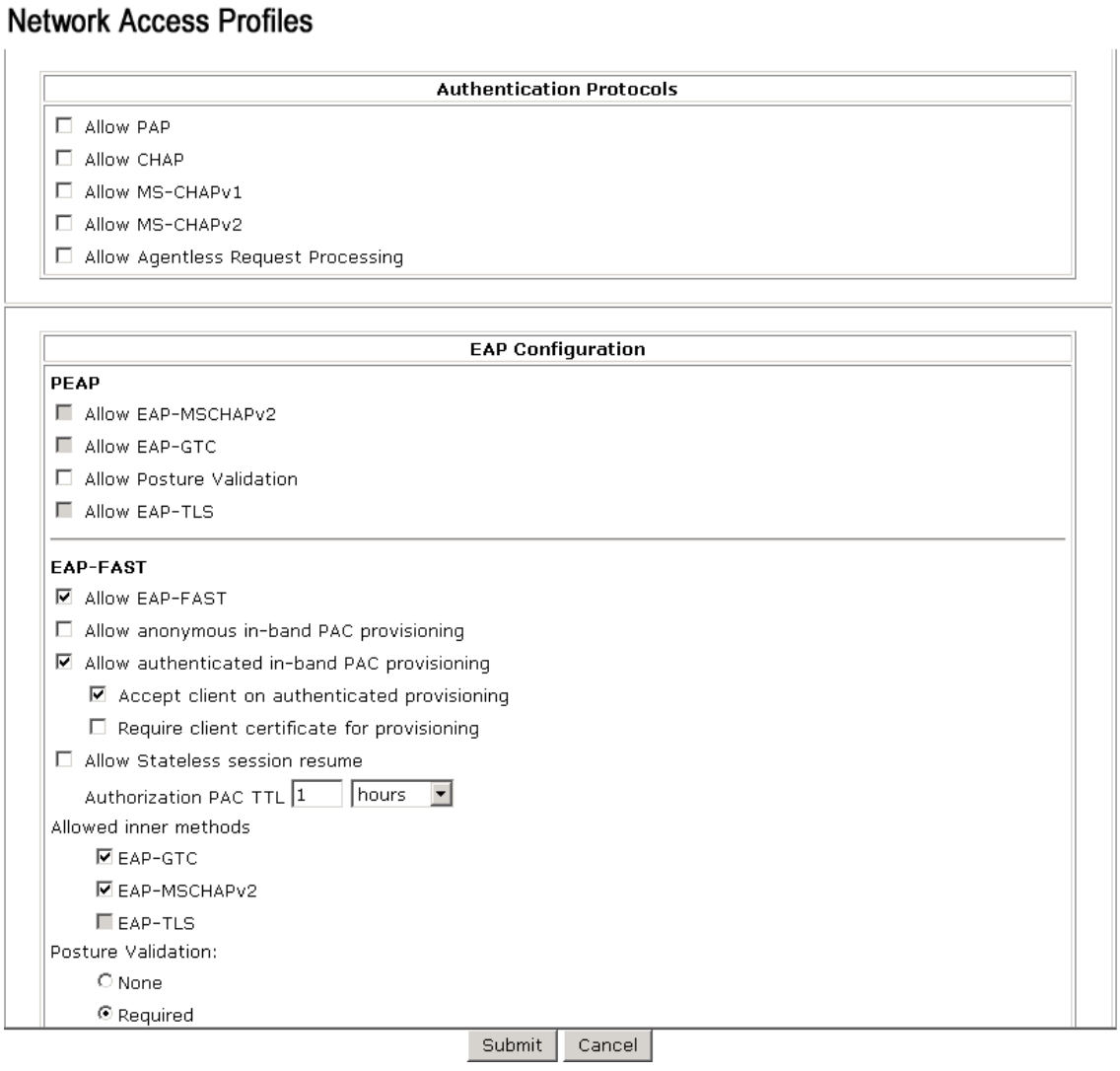
```
[026/009/001]Cisco-av-pair = aaa:service=ip admission
[006]Service-Type != 10
```

These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 9-47 shows the Protocols settings for the Wireless (NAC L2 802.1x) template.

Figure 9-47 Protocols Setting for Wireless NAC 802.1x Template



In the EAP Configuration section, Posture Validation is enabled.

Authorization Policy

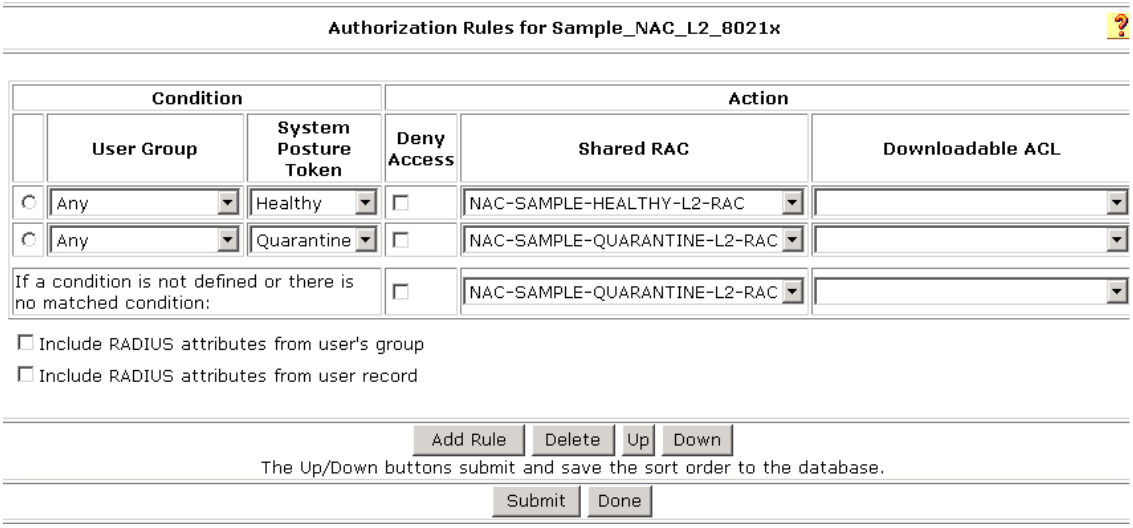
To configure an authorization policy for the Wireless NAC Layer 2 802.1x template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authorization** link from the Policies column.

The Authorization page for the profile appears, as shown in Figure 9-48.

Figure 9-48 Authorization Page for Wireless (NAC L2 802.1x) Profile Template



On this page, you can see the Wireless (NAC L2 802.1x) template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

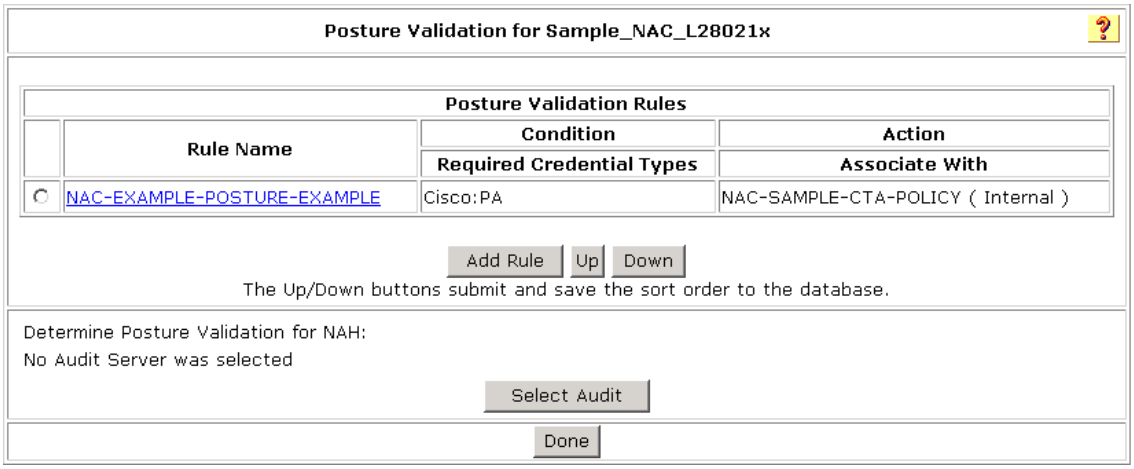
b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Sample Posture Validation Rule

Figure 9-49 shows the sample posture validation policy provided with the Wireless (NAC L2 802.1x) template.

Figure 9-49 Sample Posture Validation Policy for Wireless (NAC L2 802.1x) Template



Note The posture validation policy for the wireless NAC L2 802.1x template is the same as for the NAC L2 802.1x template.

Using a Sample Agentless Host Template

ACS 4.1 provides two sample templates for agentless host processing:

- Agentless Host for L3
- Agentless Host for L2 (802.1x fallback)

These two templates are almost identical. This section documents the steps for using the Agentless Host for Layer 3 template.

Note You can use the Agentless Host for L2 (802.1x Fallback) profile template to create a profile that matches a RADIUS request a switch sends. Once the profile is created, an analysis of the RADIUS packet that comes from the Catalyst 6500 must be done to create an accurate match for the profile. The RADIUS request from the switch has a Service Type value of 10, just like NAC-L2-IP; but does not have a Cisco Attribute Value Pair (AV pair) that contains the keyword `service`. Therefore, the template enables two entries in the Advanced Filtering section.

The Agentless Host for Layer 3 template creates a profile for Layer 3 requests that involve agentless host processing. Before you use this template, you should choose **System Configuration > Global Authentication Setup** and check the **Enable Posture Validation** check box**.**

To create an agentless host for Layer 3 profile template:

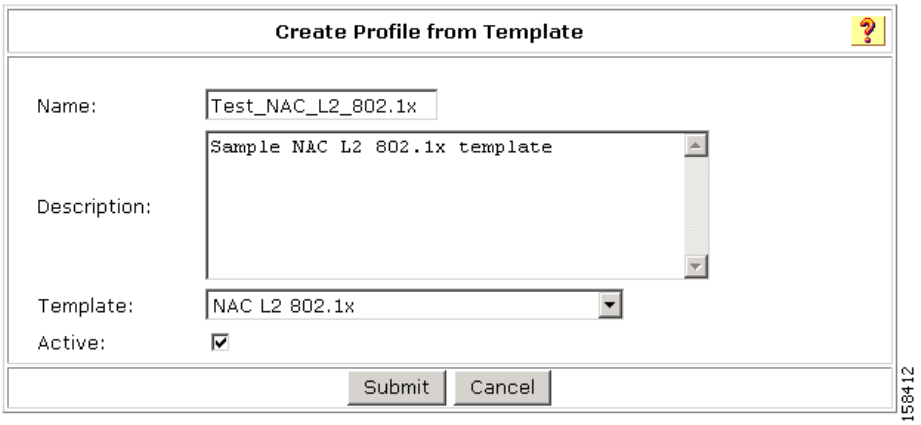
Step 1 In the navigation bar, click **Network Access Profiles**.

The Network Access Profiles page opens.

Step 2 Click **Add Template Profile**.

The Create Profile from Template page opens, as shown in Figure 9-50.

Figure 9-50 Create Profile From Template Page



Step 3 Enter a Name and Description (optional).

Step 4 From the **Template** drop-down list, choose **Agentless Host for L3**.

Step 5 Check the **Active** check box.

Step 6 Click **Submit**.

If no error appears, then you have created a profile that can authenticate Layer 3 NAC hosts.

The Edit Network Access Profile page opens, and the new profile is listed in the Name column.

The predefined values for the Agentless Host for Layer 3 template include:

- Profile Setup
- Protocols
- A sample posture validation policy
- Authentication policy

Step 7 To select a predefined set of values, click on one of the configuration options.

- The profile name (to select the profile setup page for the profile)
- Protocols
- Authentication Policy
- Sample Posture Validation Rules

Profile Setup

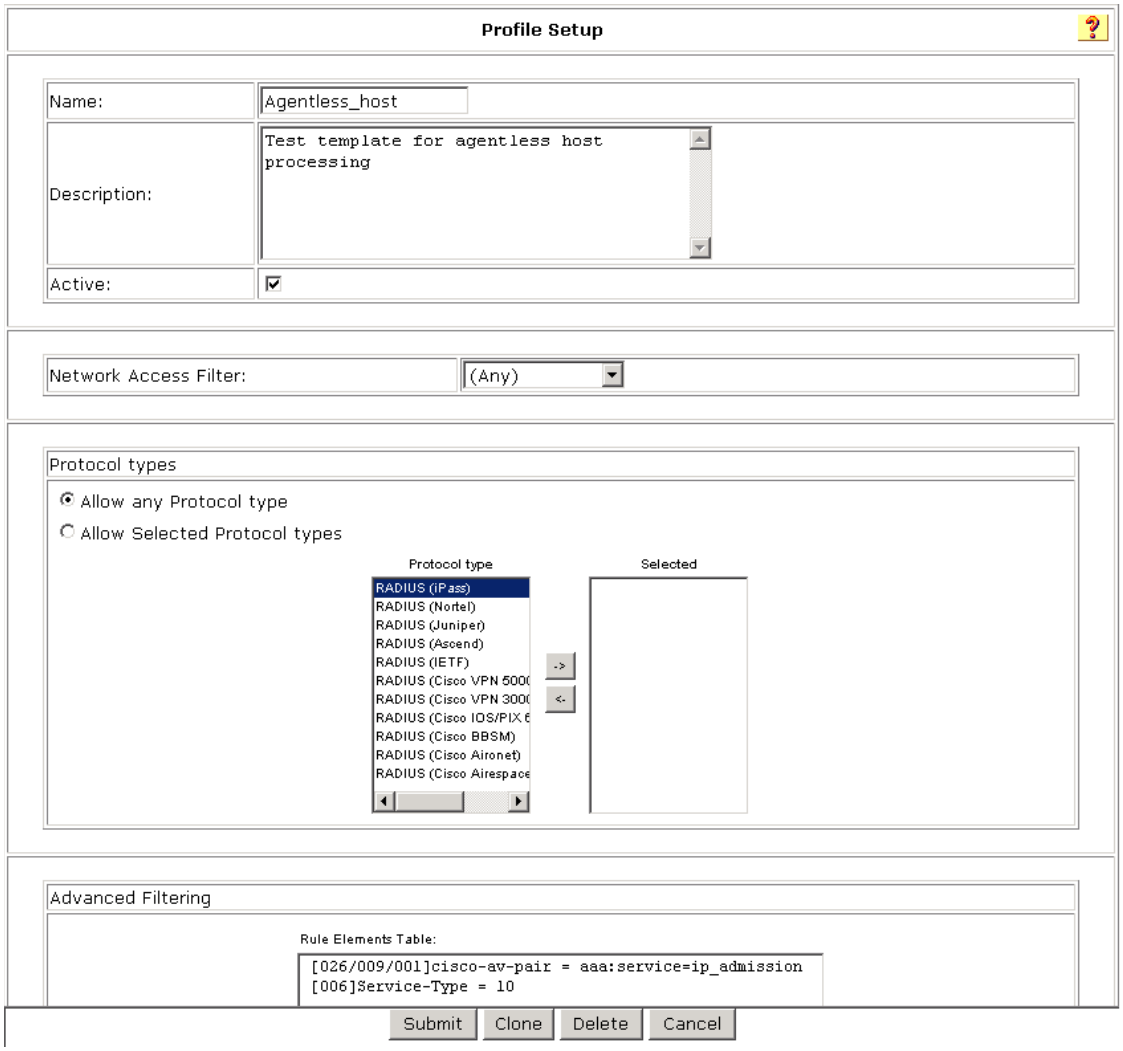
To use the Profile Setup settings from the template:

Step 1 Go to Network Access Profiles.

Step 2 Choose the profile that you created.

Step 3 The Profile Setup page appears, as shown in Figure 9-51.

Figure 9-51 Profile Setup Page for Agentless Host for Layer 3 Template



The default settings for the profile are:

- **Any** appears in the Network Access Filter field, which means that this profile has no IP filter.

  You can choose NAFs from the drop-down list, so that only specific host IPs match this profile.
- In the Protocol types list, **Allow any Protocol type** appears in the Protocol types list, which means that no protocol type filter exists for this profile.

- You can click the **Allow Selected Protocol types** option to specify a protocol type for filtering.
- Two rules are configured in **Advanced Filtering**:

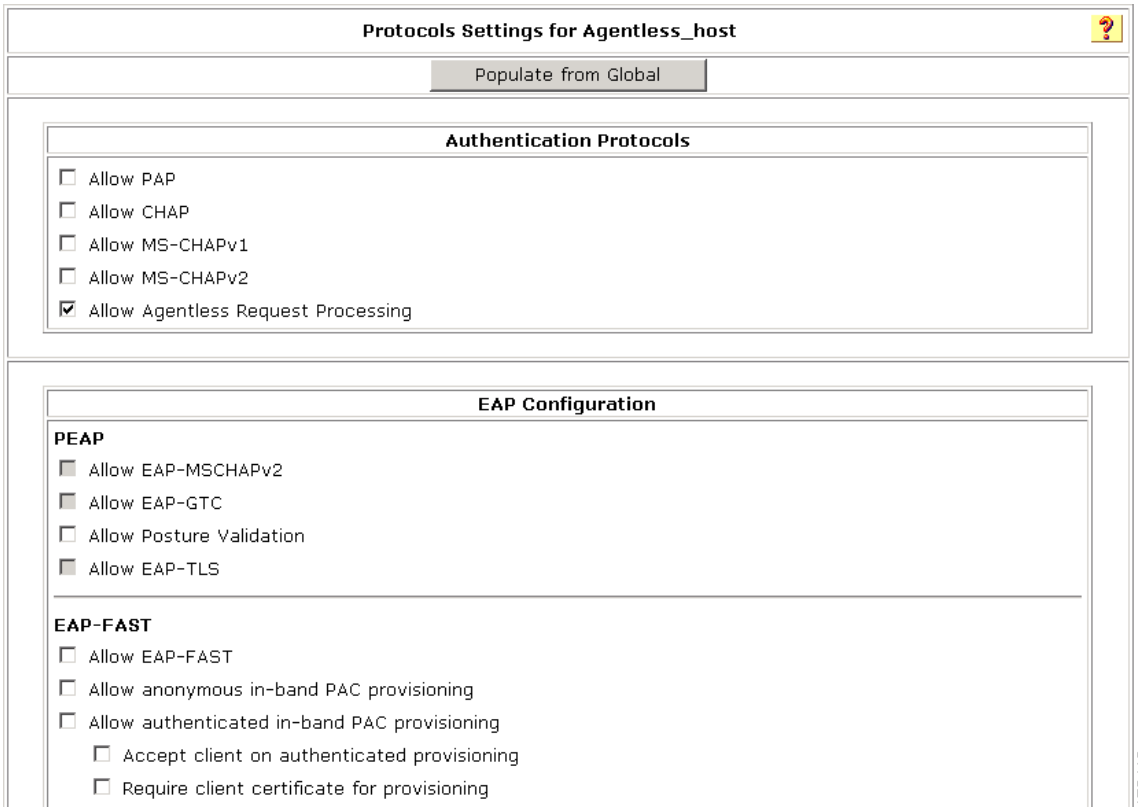
```
[026/009/001]Cisco-av-pair = aaa:service=ip admission
[006]Service-Type != 10
```

These rules specify that the associated profile policies authenticate and authorize each RADIUS request that matches the attribute's rules. You can change the advanced filter, and add, remove, or edit any RADIUS attribute that the RADIUS client sends.

Protocols Policy

Figure 9-52 shows the Protocols settings for the Agentless Host for Layer 3 template.

Figure 9-52 Protocols Setting for Agentless Host for Layer 3 Template



In the Authentication Protocols section, check Agentless Host processing.

Authentication Policy

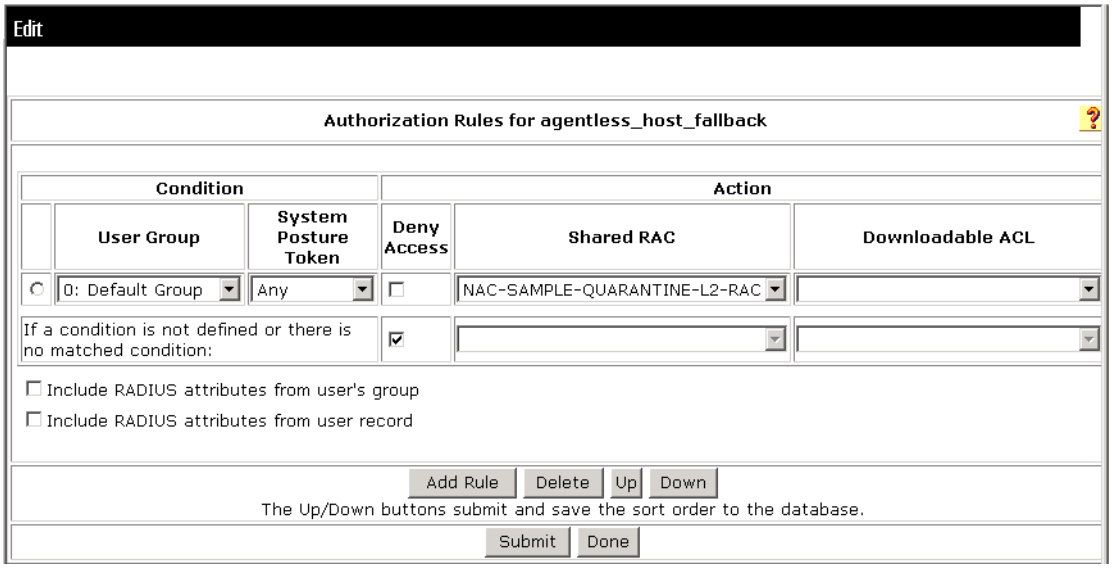
To configure an authentication policy for the Agentless Host for Layer 3 template:

Step 1 Go to **Network Access Profiles**.

Step 2 Choose the **Authentication** link from the Policies column.

The Authentication page for the profile appears, as shown in Figure 9-53.

Figure 9-53 Authentication Page for Agentless Host for Layer 3 Profile Template



On this page, you can see the Agentless Host for Layer 3 template configuration for authentication:

Step 3 Specify the external database that ACS uses to perform authentication:

a. To keep the default setting (ACS uses its internal database), click the **Internal ACS DB** radio button.

b. To specify a LDAP server, click the **LDAP Server** radio button and then, from the drop-down list, choose an LDAP server.

c. From the **If Agentless request was not assigned a user-group** drop-down list, choose a user group to which ACS assigns a host that is not matched to a user group.

Step 9: Map Posture Validation Components to Profiles

To add an internal posture validation policy, external posture validation server, or both, to a profile:

Step 1 Choose **Network Access Profiles**.

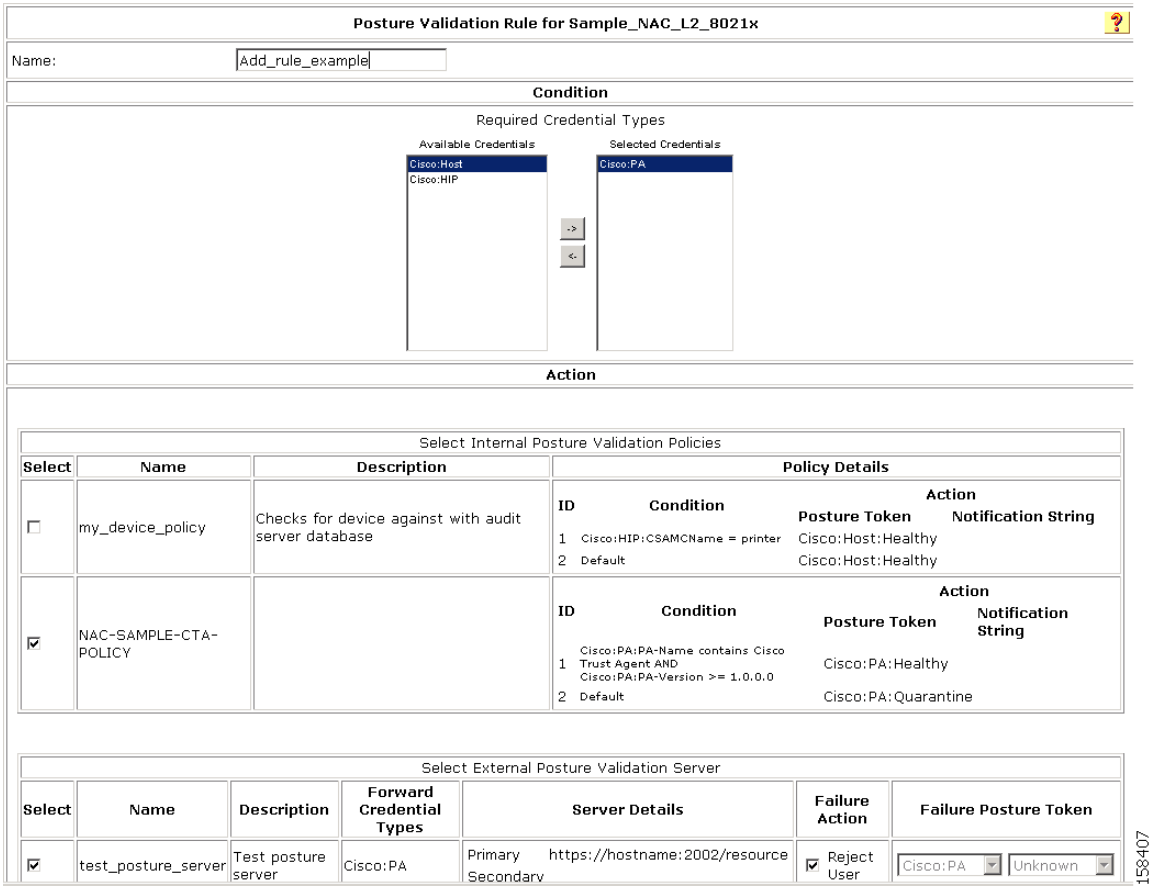
Step 2 Choose the relevant profile **Posture Validation** policy.

Step 3 Click **Add Rule**.

Step 4 Enter a Name for the rule.

The Add/Edit Posture Validation Rule page for the specified rule appears, as shown in Figure 9-54.

Figure 9-54 Add/Edit Posture Validation Rule Page



Step 5 Choose the Required Credential Types.

Step 6 In the Select External Posture Validation Sever section, select the policies or server that you want to map to this profile. To select a:

- Posture Server, check the check box next to the server name.
- Policy, check the check box next to a policy in the Failure Action column.

Step 7 Click **Submit**.

Step 8 Click **Back** to return to the Posture Validation policy.

Step 9 Click **Apply + Restart**.

Step 10: Map an Audit Server to a Profile

To add an external posture validation audit server to a profile:

Step 1 Choose **Network Access Profiles**.

Step 2 Click the **Protocols** link for the relevant Posture Validation Policy.

The Protocols Settings page for the policy that you choose opens.

Step 3 Check the **Allow Agentless Request Processing** check box.

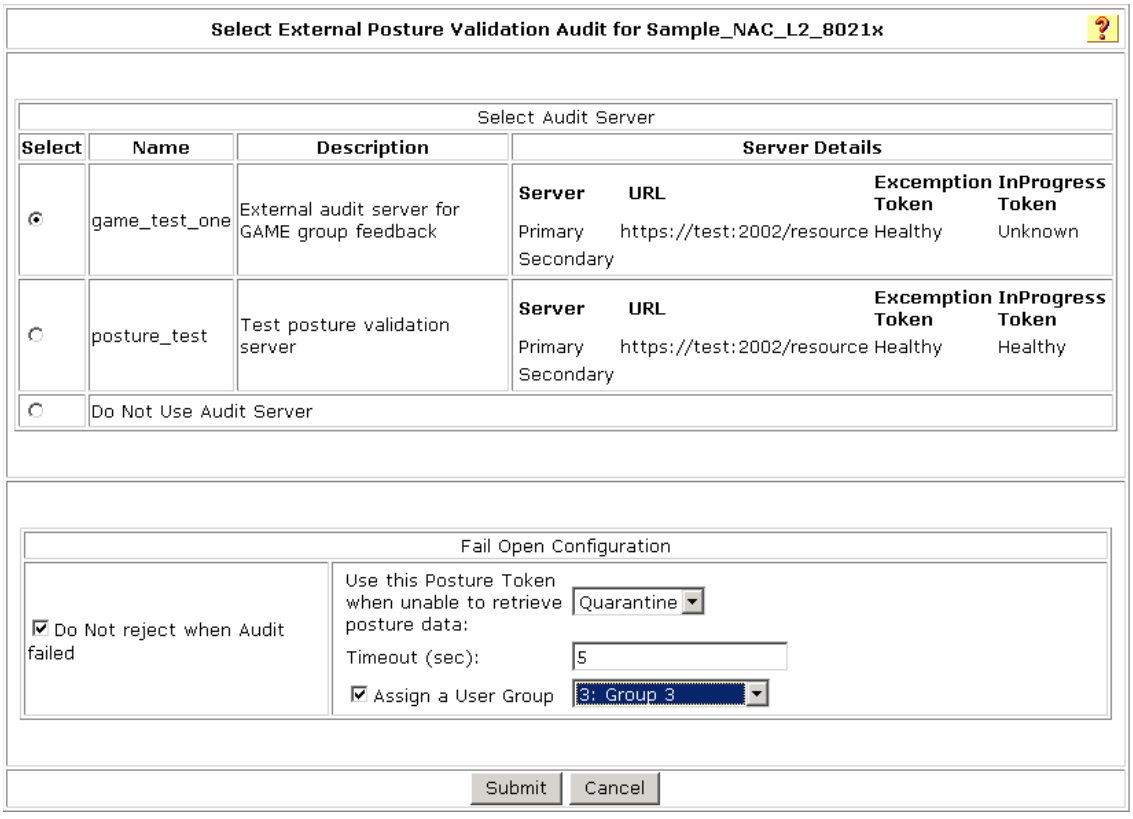
Step 4 Click **Submit**.

Step 5 Click the **Posture Validation** link for the relevant profile Posture Validation policy.

Step 6 Click **Select Audit**.

The Select External Posture Validation Audit Server page opens, as shown in Figure 9-55.

Figure 9-55 Select External Validation Audit Server Page



Step 7 Choose the audit server to use.

Step 8 To specify a Fail Open configuration to use if the audit fails:

a. Check the **Do not reject when Audit failed** check box.

b. From the Use this Posture Token when unable to retrieve posture data drop-down list, choose a posture token to apply if the audit fails.

c. Enter a timeout value in seconds.

d. If you want to specify a user group to which to assign the supplicant if the audit fails, check the **Assign a User Group** check box and then from the Assign a User Group drop-down list, choose a user group.

Step 9 Click **Submit**.

Step 10 Click **Done.**

Step 11 Click **Apply and Restart**.

Step 11 (Optional): Configure GAME Group Feedback

If you are using ACS in a NAC environment with agentless hosts, then you must configure Generic Authorization Message Exchange (GAME) group feedback.

To configure GAME group feedback:

Step 1 Import an audit vendor file by using **CSUtil**.

See Import an Audit Vendor File by Using CSUtil, page 9-73 for details.

Step 2 Import a device-type attribute file by using **CSUtil**.

See Import a Device-Type Attribute File by Using CSUtil, page 9-73 for details.

Step 3 Import NAC attribute-value pairs.

See Import NAC Attribute-Value Pairs, page 9-73 for details.

Step 4 Configure database support for agentless host processing.

The database that you use can be an external LDAP database (preferred) or the ACS internal database. See Configure Database Support for Agentless Host Processing, page 9-74 for details.

Step 5 Enable Posture Validation.

See Enable Posture Validation, page 9-74 for details.

Step 6 Configure an external audit server.

See Configure an External Audit Server, page 9-74 for details.

Step 7 Enable GAME group feedback.

To enable GAME group feedback, in the external audit server posture validation setup section, configure:

- Which hosts are audited
- GAME group feedback
- Device-type retrieval and mapping for vendors who have a device attribute in the RADIUS dictionary

See Enable GAME Group Feedback, page 9-79 for details.

Step 8 Set up a device group policy.

See Enable GAME Group Feedback, page 9-79 for details.

Import an Audit Vendor File by Using CSUtil

For information on importing an audit vendor file by using **CSUtil**, see the "Adding a Custom RADIUS Vendor and VSA Set" section in Appendix D of the *User Guide for Cisco Secure Access Control Server 4.2*, "*CSUtil Database Utility.*"

Import a Device-Type Attribute File by Using CSUtil

Before you can configure GAME group feedback, you must import an attribute file that contains a device-type attribute.

The format of a text file to set up a device-type attributes is:

```
[attr#0]
vendor-id=<the vendor identifier number>
vendor-name=<the name of the vendor>
application-id=6
application-name=Audit
attribute-id=00012
attribute-name=Device-Type
attribute-profile=in out
atribute-type=string
```

To import the file:

Step 1 Save the text file that sets up the device-type attribute in an appropriate directory.

Step 2 Open a DOS command window.

Step 3 Enter:

CSUtil -addAVP <*device-type filename*>

where *device-type filename* is the name of the text file that contains the device-type attribute.

Step 4 Restart ACS:

a. In the navigation bar, click **System Configuration**.

b. Click **Service Control**.

c. Click **Restart**.

Import NAC Attribute-Value Pairs

To import NAC attribute-value pairs:

Step 1 Use a text editor to create a NAC attribute-value pairs file.

Step 2 Import the file by using **CSUtil**. Then:

a. Start a DOS command window.

b. Enter:

CSUtil -addAVP <*NAC AV-pair filename*>

where *NAC AV-pair filename* is the name of the text file that contains the device-type attribute.

Step 3 Restart ACS:

a. In the navigation bar, click **System Configuration**.

b. Click **Service Control**.

c. Click **Restart**.

Configure Database Support for Agentless Host Processing

The database that you use can be an external LDAP database (preferred) or the ACS internal database.

For information on configuring database support for agentless host processing, see Step 4: Configure LDAP Support for MAB, page 6-10.

Enable Posture Validation

You must enable posture validation in two places. The

- Global Authentication Page, as part of the configuration for PEAP.
- EAP configuration section of the Protocols page for the NAP that enables agentless host support.

Configure an External Audit Server

For detailed instructions on configuring an external audit server, see Configure an External Posture Validation Audit Server, page 7-31.

Configure an External Posture Validation Audit Server

A NAC-enabled network might include agentless hosts that do not have the NAC client software. ACS can defer the posture validation of the agentless hosts to an audit server. The audit server determines the posture credentials of a host without relying on the presence of a PA.

Configuring an external audit server involves two stages:

- Adding the posture attribute to the ACS internal dictionary.
- Configuring an external posture validation server (audit server).

Add the Posture Attribute to the ACS Dictionary

Before you can create an external posture validation server, you must add one or more vendor attributes to the ACS internal data dictionary. To do this, you use the **bin\CSUtil** tool, which is located in the ACS installation directory.

To add the posture attributes:

Step 1 Create a text file in the *Utils* directory with the following format:

```
[attr#0]
vendor-id=[your vendor id]
vendor-name=[The name of you company]
application-id=6
application-name=Audit
attribute-id=00003
attribute-name=Dummy-attr
attribute-profile=out
attribute-type=unsigned integer
```

Your vendor ID should be the Internet Assigned Numbers Authority (IANA)-assigned number that is the first section of the posture token attribute name, [vendor]:6:

Step 2 To install the attributes specified in the text file:

a. Open a DOS command window.

b. Enter the following command:

\<*ACS_Install_Dir*>\bin\CSUtil -addAVP [*file_name*]

where *ACS_Install_Dir* is the name of the ACS installation directory and *file_name* is the name of the text file that contains vendor attributes.

Step 3 Restart the **CSAdmin**, **CSLog**, and **CSAuth** services.

Configure the External Posture Validation Audit Server

You can configure an audit server once, and then use it for other profiles.

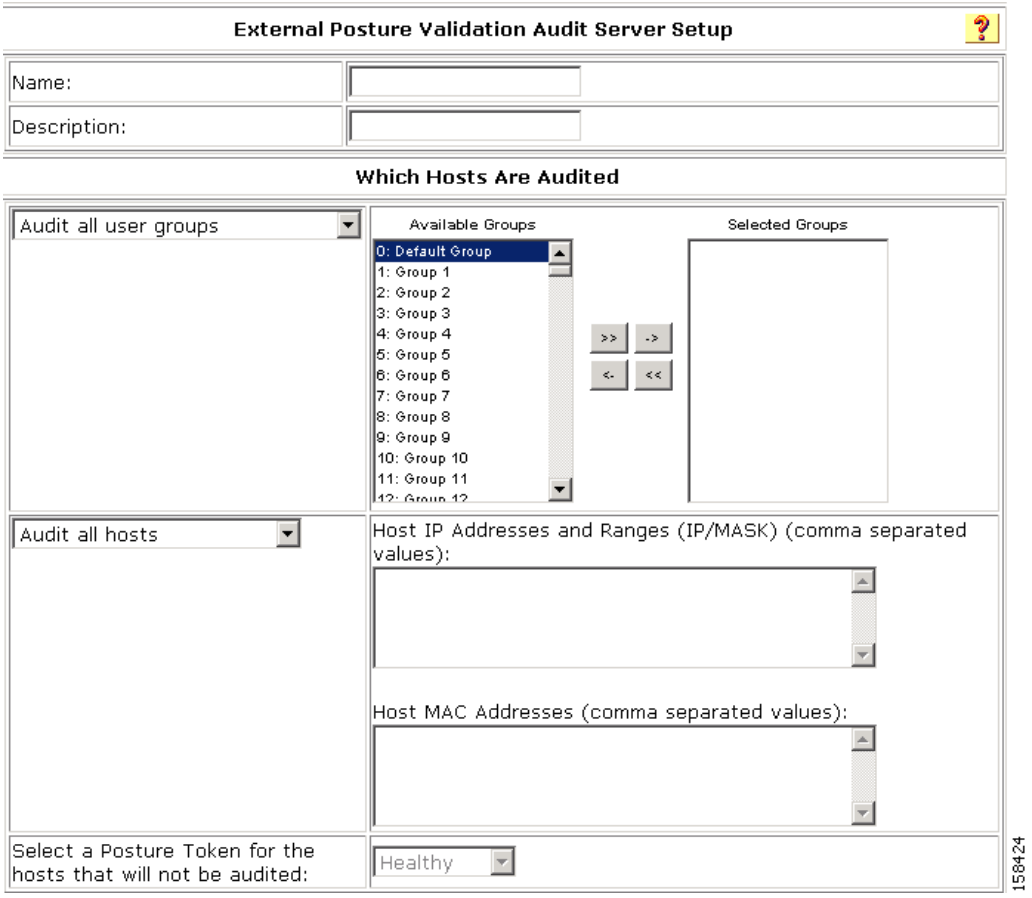
To configure an audit server:

Step 1 In the Posture Validation Components Setup page, click **External Posture Validation Audit Setup**.

Step 2 Click **Add Server**.

The External Posture Validation Audit Server Setup page appears, as shown in Figure 9-56.

Figure 9-56 External Posture Validation Audit Server Setup Page



Step 3 To configure the audit server:

a. Enter a Name and Description (optional).

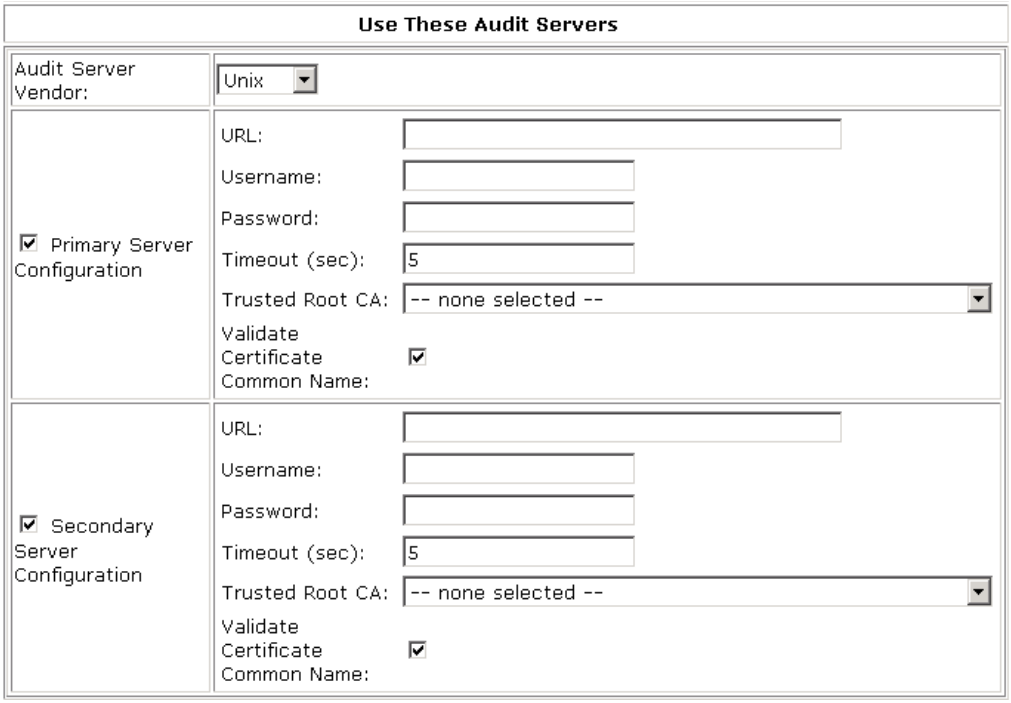
b. In the Which Hosts Are Audited section, choose what hosts you want to audit. You can enter the host IP or MAC addresses for the hosts that you want to audit or for a host that you do not want to audit.

c. For the hosts that will not be audited, choose a posture token from the drop-down list.

d. Scroll down to the Use These Audit Servers section.

Figure 9-57 shows the Use These Audit Servers section of the External Posture Validation Server Setup page.

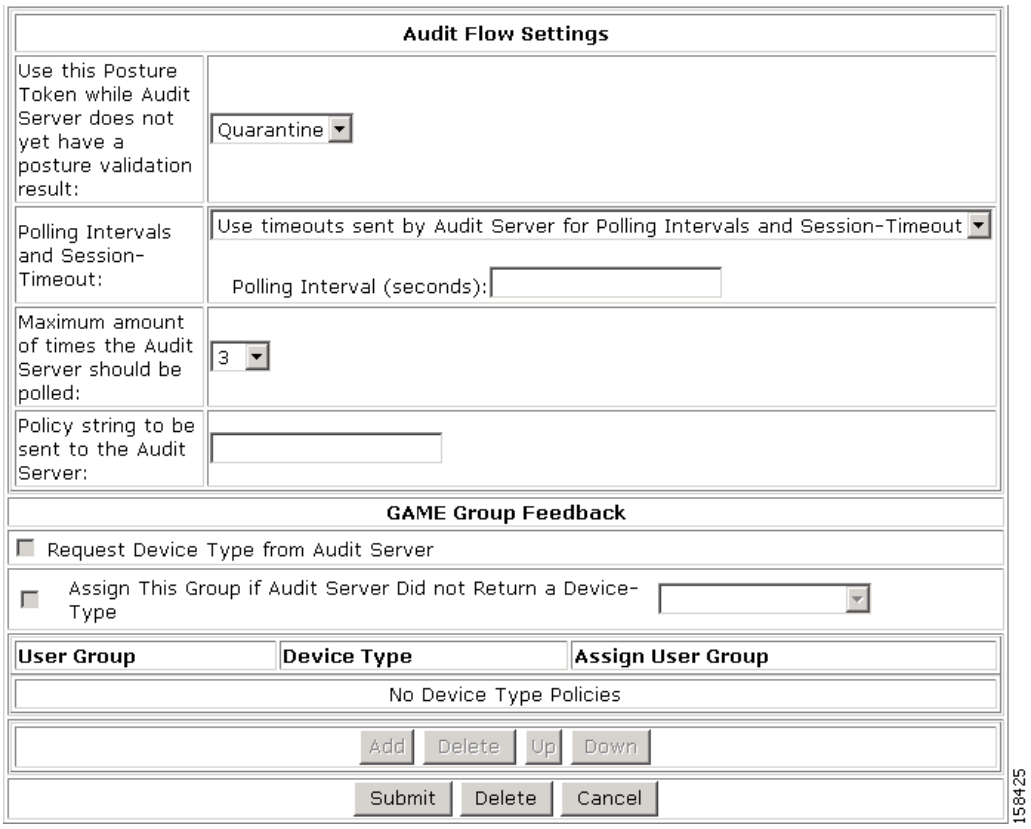
Figure 9-57 Use These Audit Servers Section



e. In the Use These Audit Servers section, enter the Audit Validation Server information, Audit Server vendor, URL, and password.

Figure 9-58 shows the Audit Flow Settings and the GAME Group Feedback section.

Figure 9-58 Audit Flow Settings and GAME Group Feedback Sections



f. If required, in the Audit Flow Setting section, set the audit-flow parameters.

g. If you are configuring GAME group feedback to support agentless host configuration in the NAC environment, configure the settings in the GAME Group Feedback section.

For information on configuring GAME Group Feedback settings, see Enable GAME Group Feedback, page 9-79.

h. Click **Submit**.

Enable GAME Group Feedback

To enable GAME group feedback:

Step 1 On the External Posture Validation Audit Server Setup page, in the GAME Group Feedback section, check the **Request Device Type from Audit Server** check box.

If this check box is not available, define an audit-device type attribute for the vendor in the internal ACS dictionary.

ACS for Windows:

With ACS for Windows, you use the **CSUtil** command. For detailed information, see "Posture Validation Attributes" in Appendix D of the *User Guide for Cisco Secure ACS*.

ACS Solution Engine:

With ACS Solution Engine, you use the NAC Attributes Management page in the web interface. See "NAC Attribute Management (ACS Solution Engine Only)" in Chapter 8 of the *User Guide for Cisco Secure ACS* for more information.

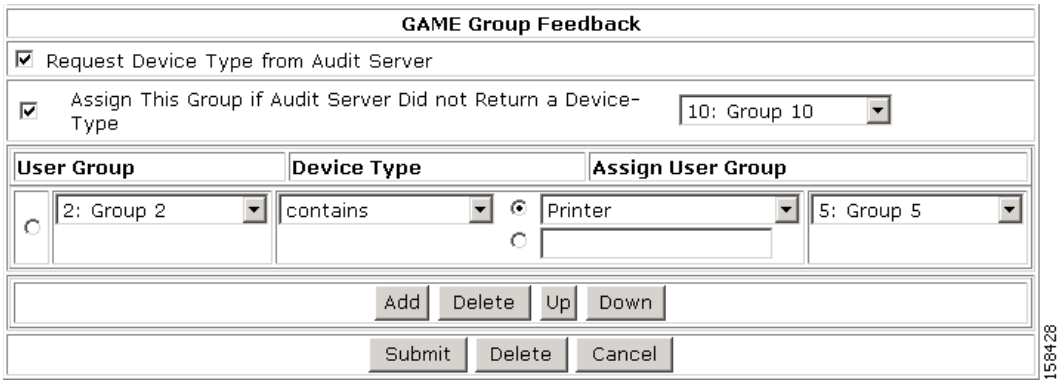
Step 2 If you want to configure a default destination group that ACS uses if the audit server does not return a device type, check the **Assign This Group if Audit Server Did not Return a Device-Type** check box.

You should now add entries to the group assignment table. The group assignment table is a list of rules that set conditions that determine the user group to which to assign a particular device type that the audit server returns.

Step 3 Click **Add** to display the group assignment table and add a device-type feedback rule.

The group assignment table appears, as shown in Figure 9-59.

Figure 9-59 GAME Group Feedback Section with Group Assignment Table



Step 4 In the group assignment table, specify:

- **User Group**—Lists all user groups, including **Any**. The device type that the MAC authentication returns is initially compared with this list of device types.
- **Match Condition**—Valid values for the operator are:
  - match-all
  - =
  - ! =

  - contains
  - starts-with
  - regular-expression
- **Device Type**—Defines the comparison criteria for the User Group by using an operator and device type. Valid values for the device type drop-down list include:
  - Printer
  - IP Phone
  - Network Infrastructure
  - Wireless Access Point
  - Windows
  - UNIX
  - Mac
  - Integrated Device
  - PDA
  - Unknown

Note Type a device type in the text box if the device type drop-down does list not contain a particular device.

- **Assign User Group**—A drop-down list of administrator-defined user groups. If the comparison of the initial User Group with the Device Type succeeds, ACS will assign this user group.

Step 5 To add additional policies, click **Add**.

Step 6 To delete a policy, highlight the policy and click **Delete**.

Step 7 To move the policies up and down in the group assignment table, click the **Up** and **Down** buttons.

Step 8 When you finish setting up policies for group assignment, click **Submit**.

Step 9 Click **Apply and Restart.**

GLOSSARY

A

AAA Authentication, Authorization, and Accounting server.-(Authentication, authorization, and accounting is pronounced “triple-A.” An AAA server is the central server that aggregates one or more authentication, authorization, or both decisions into a single system-authorization decision, and maps this decision to a network-access profile for enforcement on the NAD.

Access -Accept Response packet from the RADIUS server notifying the access server that the user is authenticated. This packet contains the user profile, which defines the specific AAA functions assigned to the user.

Access-Challenge Response packet from the RADIUS server requesting that the user supply additional information before being authenticated.

Access-Request Request packet that the access server sends to the RADIUS server requesting authentication of the user.

Accounting Accounting in network management subsystems is responsible for collecting network data relating to resource usage.

Agentless host processing A method that ACS uses to process authentication requests from hosts that do not have an authentication agent installed, such as Cisco Trust Agent.

ACL Access Control List-Each ACL consists of a set of ACL entries.

ACE Access Control Entry-An ACL Entry contains a type, a qualifier for the user or group to which the entry refers, and a set of permissions. For some entry types, the qualifier for the group or users is undefined.

APT Application Posture Token-The result of a posture validation check for a given vendor’s application.

Audit server A server that can determine the posture credentials of a host without relying on the presence of a PA on the host. The server must be able to determine the posture credentials of a host and act as a posture-validation server.

Authentication In network management security, the verification of the identity of a person or a process.

AV pair Attribute-value pair-Encoding that the RADIUS protocol uses to specify an action that the host performs when a condition represented by the attribute value is met.

C

Cisco Trust Agent Cisco Trust Agent. The Cisco implementation of the PA.

E

EAP Extensible Authentication Protocol-Provides the ability to deploy RADIUS into Ethernet network environments. EAP is defined by Internet Engineering Task Force (IETF) RFC 2284 and the IEEE 802.1x standards.

EAP-TLS Extensible Authentication Protocol-Transport Layer Security-Uses the TLS protocol (RFC 2246), which is the latest version of the Secure Socket Layer (SSL) protocol from the IETF. TLS provides a way to use certificates for user and server authentication and for dynamic session key generation.

Endpoint Device Any machine that attempts to connect to or use the resources of a network. Also referred to as a host.

External Posture Validation Server A Cisco or third-party server used to perform posture validation. A posture-validation server acts as an application-specific policy decision point in NAC for authorizing a set of posture credentials against a set of policy rules.

G

GAME group feedback Generic Authorization Message Exchange-A Cisco protocol that is used in the Cisco Network Admission Control (NAC) environment. GAME group feedback provides an added security check for MAC address authentication by checking the device type categorization that ACS determines by associating a MAC address with a user group against information stored in a database on an audit server

H

Health Registration Authority A Microsoft certificate server that obtains health certificates on behalf of NAP clients from a public key infrastructure (PKI).

HCAP Cisco Host Credentials Authorization Protocol. A protocol that ACS uses to communicate with a Microsoft NPS.

Host Another name for an endpoint device.

L

LDAP Lightweight Directory Access Protocol-A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler.

M

MAB MAC authentication bypass-An authentication method that uses the MAC address of a device to authenticate the device, instead of using an IP address.

N

NAC Network Admission Control-NAC is a Cisco-sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources; thereby limiting damage from viruses and worms. NAC is part of the Cisco Self-Defending Network, an initiative to increase network intelligence in order to enable the network to automatically identify, prevent, and adapt to security threats.

NAC/NAP Cisco Network Access Control/Microsoft Network Access Protection.

NAC-compliant applications Applications that integrate with the NAC client. Examples of such applications are Cisco Security Agent and antivirus programs that provide the NAC client with attributes about themselves, such as the version number of a virus definition file.

NAD Network Access Device-A network access device acts as a policy-enforcement point for the authorized network-access privileges that are granted to a host.

NAF Network Access Filter-A NAF is a named group of any combination of one or more of the following network elements: IP addresses, AAA clients (network devices), and network device groups (NDGs).

Using a NAF to specify a downloadable IP ACL or Network Access Restriction based on the AAA clients by whom the user may access the network saves you the effort of listing each AAA client explicitly.

NAP agent A process running on a NAP client that sends SoHs or health certificates to ACS.

NAP client A computer running Windows Vista or Windows Server 2008. NAP clients send their health credentials as Statements of Health (SoHs) or a health certificate.

NDG Network Device Group-A collection of network devices that act as a single logical group.

NPS Network Policy Server. A Microsoft server that validates health certificates from NAP clients and provides remediation instructions if needed.

P

PA Posture Agent-An application that serves as the single point of contact on the host for aggregating posture credentials from potentially multiple posture plug-ins and communicating with the network.

PAC Protected Access Credential-A security credential that is used with EAP-FAST (Flexible Authentication via Secure Tunneling). With EAP-FAST, instead of using a certificate, mutual authentication is achieved by using a PAC, which can be managed dynamically by the authentication server. The PAC can be provisioned (distributed one time) to the client either manually or automatically. Manual provisioning is delivery to the client via disk or a secured network distribution method. Automatic provisioning is an in-band, over the air, distribution.

PDP Policy Decision Point-Provides facilities for policy management and conditional filters.

PEP Policy Enforcement Point-ACS acts as the policy enforcement point for policy management.

PEAP Protected Extensible Authentication Protocol-An 802.1x authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft that Cisco Systems, Microsoft, and RSA Security submitted to the IETF.

Posture credentials State information of a network endpoint at a given point in time that represents hardware and software (OS and application) information.

Posture plug-in A third-party DLL that provides host posture credentials to a posture agent on the same endpoint for endpoint posture validation and network authorization.

PV Posture Validation-Posture validation validates the collection of attributes that describe the general state and health of the user's machine (the "host").

PVS Posture Validation Server-A posture-validation server acts as an application-specific policy-decision point in NAC for authorizing a set of posture credentials against a set of policy rules.

R

RAC RADIUS Attribute Component.

RADIUS A widely deployed protocol enabling centralized authentication, authorization, and accounting for network access.

S

SoH Statement of Health. A message that a NAP client sends to an NPS indicating the health of the client.

V

VSA Vendor Specific Attribute-Most vendors use the VSA to support value-added features.

INDEX

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

P

R

S

T

U

V

W